



ТЕХНОЛОГИИ «КИБЕРПЛАТ» (CYBERPLAT®):
ОСНОВА ГЛОБАЛЬНОЙ ИНФРАСТРУКТУРЫ
НОВОЙ ЭКОНОМИКИ

Крупнейшая система электронных платежей:
более 1 480 000 пунктов

СОДЕРЖАНИЕ

ВСТУПЛЕНИЕ.....	9
Обращение руководителя.....	10
Глоссарий.....	11
 КЛЮЧЕВАЯ РОЛЬ РЫНКА ОНЛАЙН-ПЛАТЕЖЕЙ В СОВРЕМЕННОЙ ЭКОНОМИКЕ.....	13
Для чего нужна банковская система.....	14
Требования новой экономики.....	14
Современная банковская система и требования новой экономики.....	15
Необходимость менее затратной финансовой инфраструктуры.....	16
Платёжные технологии «КиберПлат» (CyberPlat®) вне конкуренции.....	16
Невозможность удовлетворить некоторые требования без низкозатратной финансовой инфраструктуры.....	17
Затраты на производство скретч-карт и инфраструктуру их распространения.....	18
Мелкие платежи.....	19
Надёжная технология.....	19
Почему это популярно.....	20
 О КОМПАНИИ.....	21
Общие сведения.....	22
Награды партнёров.....	23
Основные показатели.....	24
 ОТЗЫВЫ Партнёров о системе «КиберПлат» (CyberPlat®).....	25
 КАК РАБОТАЕТ «КИБЕРПЛАТ» (CYBERPLAT®).....	27
Схема организации бизнеса «КиберПлат» (CyberPlat®).....	28
Партнёры компании.....	29
Технология «КиберПлат» (CyberPlat®): схема типового решения на примере domestic top-up.....	33
Модель работы «КиберПлат» (CyberPlat®).....	35
Банки — партнёры системы «КиберПлат» (CyberPlat®).....	38
Сеть приёма платежей (крупнейшие ритейлеры).....	39
География бизнеса «КиберПлат» (CyberPlat®).....	40
Социальная миссия системы электронных платежей «КиберПлат» (CyberPlat®).....	42
 ПРЕИМУЩЕСТВА ТЕХНОЛОГИЙ «КИБЕРПЛАТ» (CYBERPLAT®).....	43
Опыт и квалифицированные кадры.....	44
Безопасность и защищённость.....	45
Аппаратная многоплатформенность.....	46
Повышенная отказоустойчивость и производительность.....	47
Круглосуточная техническая поддержка.....	48
Законность и неоспоримость операций.....	48
Сертифицированность.....	48

Отсутствие конкуренции с собственными партнёрами (платёжными агентами).....	49
Отсутствие практики продвижения собственного бренда за счёт брендов партнёров.....	50
Отсутствие практики продвижения и навязывания своим партнёрам ненужных или невыгодных продуктов и сервисов.....	50
Материальная ответственность IT-персонала.....	51
Устойчивость и масштабируемость технической платформы.....	52
«КиберПлат» (CyberPlat®) работает всегда!.....	53
Проверка получателя.....	53
Онлайн (2 секунды).....	54
 ПРОДУКТЫ И РЕШЕНИЯ «КИБЕРПЛАТ» (CYBERPLAT®).....	55
Продукты и решения для ритейла.....	56
Организация приёма платежей (domestic top-up).....	56
Организация приёма платежей на предприятиях ритейла. Почему это выгодно.....	57
Как правильно организовать приём платежей в ритейле.....	58
Сервис «Сдача на телефон».....	61
Приём платежей с помощью штрих-кода.....	64
Программное решение «Модуль платежей» для персональных компьютеров.....	65
Решение для подключения к приёму платежей касс торговых предприятий.....	65
Получение прибыли от совместного брендинга (co-branding) «КиберСдача» — уникальный финансовый сервис.....	66
Общая схема зачисления сдачи.....	67
Решения для банков.....	70
Предложение «КиберПлат» (CyberPlat®) для банков.....	70
Интеграция эквайринга платёжных карт и приёма наличных платежей.....	71
Приём платежей.....	73
Автоплатежи — готовое решение для банков.....	74
Продукты и решения для терминальных сетей.....	78
Организация приёма платежей в терминальных сетях.....	78
Программный комплекс «Терминал Клиент 3.0.x.x».....	79
Технический сервис «Мониторинг терминалов».....	81
Технологическое решение «Реклама на терминалах».....	82
Решения для микрофинансовых организаций.....	83
Приём платежей за погашение займов.....	83
Выдача займов на банковские карты.....	85
Сервис упрощённой идентификации физических лиц.....	85
Сервис рейтинговой информации.....	85
Эквайринг — оплата займов на веб-ресурсах МФО.....	86
Банковские продукты.....	87
Универсальные шлюзы.....	87
Платёжи по свободным реквизитам.....	87

Банковский провайдер.....	89
Пополнение банковских счетов.....	89
Отраслевые продукты «КиберПлат» (CyberPlat®).....	90
«Страхование» (решения для страхового рынка).....	90
«Парковки» (решение по автоматизации парковок).....	92
«Торговые сети» (решение по увеличению посещаемости предприятий ритейла).....	95
SaaS (оплата программного обеспечения за время пользования).....	97
Интегратор систем денежных переводов.....	101
КУБ: Канал удалённый банковский.....	108
International top-up: международные операторы и трансграничные платежи.....	113
Решения в сфере мобильной коммерции.....	114
CyberPay.....	114
Технология CyberDeN — уникальный инструмент мобильной коммерции.....	116
Онлайн-инкассация.....	123
 ДОПОЛНИТЕЛЬНЫЕ СЕРВИСЫ ДЛЯ ПАРТНЁРОВ	
«КИБЕРПЛАТ» (CYBERPLAT®).....	127
Скоринг по номеру телефона.....	128
Целевое SMS-информирование.....	128
Мониторинг транзакций в режиме онлайн.....	129
Онлайн-кредитование.....	130
Продукты B2C.....	130
Plat.ru — «Платёжная книжка КиберПлат».....	130
Сервис TopUp.ru.....	136
Виртуальная предоплаченная карта VISA Virtuon.....	136
Пополнение карт VISA, MasterCard, МИР в сети «КиберПлат» (CyberPlat®).....	138
 КАК СТАТЬ ПАРТНЁРОМ «КИБЕРПЛАТ» (CYBERPLAT®).....	
Стань агентом системы «КиберПлат» (CyberPlat®) за 5 минут!	139
Автоматическая регистрация агентов.....	140
Стань Региональным представителем системы электронных платежей «КиберПлат» (CyberPlat®)!	141
 CYBERFT — УДОБНАЯ И БЕЗОПАСНАЯ СИСТЕМА	
ОБМЕНА ФИНАНСОВЫМИ СООБЩЕНИЯМИ.....	143
Платформа CyberFT.....	144
SWIFT: существующие ограничения.....	144
Новый подход к обмену финансовыми сообщениями.....	146
CyberFT, SWIFT и СПФС.....	148
Многопровайдерность.....	152
Универсальность.....	157

Безопасность.....	158
Поддерживаемые форматы, гибкость и вариативность развития.....	159
Взаимодействие со SWIFT. Простая интеграция для банков.....	161
Доступность.....	163
Конкурентоспособность.....	165
Текущая ситуация с расчётами в РФ.....	166
Требования к программному обеспечению.....	167
Терминал CyberFT.....	168
CyberFT: одна система для решения множества задач.....	170
Универсальное решение для взаимодействия корпоративных клиентов с банками.....	171
Универсальный Host-to-Host.....	172
Межбанковский Cash Pooling.....	173
Платёжный модуль CyberFT 1C.....	174
Схема работы через ERP.....	176
Юридически значимый межкорпоративный электронный документооборот.....	177
Основные преимущества CyberFT.....	178
Эффект от внедрения CyberFT.....	179
Платформа CyberFT для органов власти, ведомств, государственных и частных компаний.....	181
Текущая ситуация со внутри- и межведомственным документооборотом в России.....	181
Платформа CyberFT — элемент национальной безопасности и гарант сохранности важной государственной информации.....	182
Инструмент исполнения локального законодательства.....	184
Средство безопасного информационного обмена.....	184
Основные стратегические принципы и возможности сети CyberFT.....	185
Отличительные признаки сети CyberFT.....	186
 «КИБЕРСДАЧА» — УНИКАЛЬНЫЙ ФИНАНСОВЫЙ СЕРВИС	
ДЛЯ РИТЕЙЛА, БАНКОВ, ПРОВАЙДЕРОВ УСЛУГ.....	193
Суть продукта.....	194
Карта «КиберСдача».....	194
Общая схема зачисления.....	195
Преимущества отказа от использования мелочи (монет и мелкой купюры) при сдаче.....	196
Преимущества уникального финансового сервиса «КиберСдача».....	197
Оценка эффективности.....	198
Рост оборота высокомаржинальных товаров.....	202
Зачисление сдачи.....	204
Как активировать карту.....	205
Как выглядит карта «КиберСдача».....	207
Виртуальная карта «КиберСдача».....	208
Эмиссия карт «КиберСдача».....	208

Карта «КиберСдача», предактивированная эмитентом-провайдером.....	209
Привязка карты «КиберСдача» к программе лояльности торговой сети.....	210
Карта «КиберСдача хэви».....	211
Предложения для рекламодателей.....	212
Преимущества для провайдеров-эмитентов, выпускающих карты «КиберСдача» со своим логотипом.....	214
Преимущества для банков-эмитентов, выпускающих карты «КиберСдача» со своим логотипом.....	215
Преимущества для эмитентов-рекламодателей, выпускающих карты «КиберСдача» со своим логотипом.....	216
Массовая эмиссия карт.....	217
Дополнительные возможности для развития бизнеса.....	219
Комиссионная политика.....	221
Преимущества для участников проекта.....	221
ТЕХНОЛОГИИ ГЛОБАЛЬНОГО ЭЛЕКТРОННОГО БИЗНЕСА.	
МЕЖДУНАРОДНЫЕ ПРОЕКТЫ «КИБЕРПЛАТ» (CYBERPLAT®).....	223
CyberPlat India — один из лидеров национального финтех рынка.....	224
Общие сведения.....	224
Продукты и решения.....	225
«КиберПлат Казахстан» — основоположник рынка электронных расчётов в Республике Казахстан.....	228
Общие сведения.....	228
Клиентская база.....	229
Преимущества для клиентов и партнёров.....	230
Инновационные сервисы «КиберПлат» (CyberPlat®) для зарубежных операторов связи.....	231
Предложения для зарубежных операторов связи.....	231
Аппаратная многоплатформенность.....	231
Безопасность платежей.....	232
Преимущества «КиберПлат» (CyberPlat®) перед другими платёжными технологиями.....	232
Преимущества от внедрения платёжных решений «КиберПлат» (CyberPlat®).....	234
КОНТАКТЫ ООО «КИБЕРПЛАТ».....	235
ПРИЛОЖЕНИЕ.....	
Технологии платежей.....	238
CyberCheck.....	238
CyberCheck с использованием банковских пластиковых карт.....	240
CyberPlatPay.....	242
Риск-менеджмент криптовалют.....	244

ВСТУПЛЕНИЕ

ГРИБОВ АНДРЕЙ ЮРЬЕВИЧ
Генеральный директор ООО «КИБЕРПЛАТ»

Более полутора десятилетий назад Россия вошла в XXI век — век экономики знаний, и система «КиберПлат» (CyberPlat®) возникла и развивается в ответ на возросшие потребности бизнеса третьего тысячелетия. Появление новых сервисов и услуг, максимально доступных для всё более широких слоёв населения, требуют создания новых платёжных инструментов.

В своё время банки создавались для хранения больших сумм денег. Поэтому банки имеют укреплённые стены, бронированные двери, обслуживаются высококвалифицированным и, соответственно, высокооплачиваемым персоналом, а также используют лучшие технические достижения для обеспечения сохранности денег. В результате себестоимость транзакции по приёму наличных денег и проведению платежа обычно составляет не менее \$1.

Экономика знаний создала множество коммерческих предприятий (например, предоставляющих услуги связи), которые обслуживают десятки миллионов абонентов. Эти предприятия собирают очень большое количество мелких платежей. Средняя величина транзакции в системе «КиберПлат» (CyberPlat®) в России составляет всего около \$8,5. Проведение таких мелких платежей для банков не выгодно.

Вместе с тем для процедуры приёма подобных сумм не нужны высокие степени безопасности. Платёжи размером в несколько долларов США вполне безопасно собирать через кассы обычных ритейловых сетей (салоны связи, супермаркеты, аптеки, АЗС), что намного дешевле. Сегодня частные клиенты осуществляют регулярные мелкие платежи — за связь, интернет, кабельное ТВ — преимущественно именно через ритейловые сети. Кроме того, с изменением законодательства в ритейл перемещаются и другие операции, такие, как погашение банковских кредитов и пополнение банковских счетов, оплата штрафов ГИБДД и налогов, отправка денежных переводов, внесение квартплаты и оплата коммунальных услуг. На конец 2018 года в системе электронных платежей «КиберПлат» (CyberPlat®) было зарегистрировано свыше 8 тысяч получателей платежей — поставщиков товаров и услуг.

«КиберПлат» (CyberPlat®) помогает своим партнёрам, участникам системы электронных платежей получить новые источники заработка и увеличить оборот по профильному виду бизнеса.

Для этого мы создали и развиваем мощную платёжную инфраструктуру. Уже сегодня она многократно превосходит всю банковскую систему страны по числу пунктов приёма платежей.

ОПЕРАТОР — любая организация, предоставляющая услуги населению и принимающая оплату через «КиберПлат» (CyberPlat®). Это компании мобильной и фиксированной связи (МТС, Билайн, МегаФон, Tele2, «Ростелеком» и др.), провайдеры коммерческого ТВ (НТВ+, Акадо и др.), провайдеры доступа в интернет и IP-телефонии (Qwerty, Дом.ру и др.), предприятия ЖКХ и энергетики, службы продажи авиабилетов и т.д.

АБОНЕНТ — любое физическое или юридическое лицо, осуществляющее оплату услуг операторов через «КиберПлат» (CyberPlat®) либо в rpreaid-режиме (операция пополнения лицевого счёта), либо в виде абонентской платы, либо в форме платежа за уже предоставленные услуги, к примеру, коммунальные.

ПУНКТ ПРИЁМА ПЛАТЕЖЕЙ — любое рабочее место, на котором налажен приём платежей абонентов в пользу операторов через «КиберПлат» (CyberPlat®) — касса магазина, платёжный терминал, рабочее место кассира банка или менеджера салона связи, продавца торгового киоска и т.п.

КАССИР — специалист пункта приёма платежей, непосредственно обслуживающий абонента.

ТОРГОВЫЕ СЕТИ — совокупность пунктов приёма платежей, объединённых одним брендом (к примеру, сеть салонов связи «Евросеть», розничная сеть салонов МТС, сеть магазинов «Эльдорадо»). Торговой сетью также считается и крупный универсам с десятком касс, каждая из которых является пунктом приёма платежей.

ПЛАТЁЖНЫЙ ТЕРМИНАЛ (SELF-SERVICE CASH-IN-KIOSK) — полностью автоматизированный пункт приёма платежей, работающий без кассира, — аналог банкомата. Известны платёжные терминалы таких сетей, как «Элекснет», «ПлатёжКа», «Плат-Форма» и т.д.

ПЛАТЁЖНЫЙ АГЕНТ (АГЕНТ) — юридическое лицо (торговая сеть или одиночный пункт приёма платежей, например, магазин, киоск, аптека) или индивидуальный предприниматель, принимающие платежи абонентов через «КиберПлат» (CyberPlat®) в пользу провайдеров услуг.

БАНКОВСКИЙ ПЛАТЁЖНЫЙ АГЕНТ — юридическое лицо, за исключением банков, или индивидуальный предприниматель, которые привлекаются банком для оказания платёжных услуг через систему «КиберПлат» (CyberPlat®).

РЕГИОНАЛЬНЫЙ ПРЕДСТАВИТЕЛЬ — представитель компании «КиберПлат» (CyberPlat®), занимающийся привлечением новых агентов системы электронных платежей. Доход представителей формируется за счёт комиссионного вознаграждения, размер которого прямо зависит от оборота привлечённых агентов.

КЛЮЧЕВАЯ РОЛЬ РЫНКА ОНЛАЙН-ПЛАТЕЖЕЙ В СОВРЕМЕННОЙ ЭКОНОМИКЕ

ДЛЯ ЧЕГО НУЖНА БАНКОВСКАЯ СИСТЕМА



Торговля может функционировать эффективно только в условиях хорошо развитой банковской сети. Однако инфраструктура действующей банковской системы не отлажена для проведения мелких транзакций. Банки традиционно используются как место для безопасного хранения денег, а также перевода крупных денежных сумм. Неотъемлемыми атрибутами банковских учреждений являются крепкие стены, пуленепробиваемые окна, вооружённая охрана и высокопрофессиональный персонал.

В силу этих причин себестоимость розничной банковской операции весьма велика. Процедура осуществления платежей также является затратной по времени как для клиента, так и для высокооплачиваемого банковского персонала. В связи с этим розничный платёж в банке не может быть дешёвой операцией, и её себестоимость для кредитного учреждения составляет не менее \$1.

ТРЕБОВАНИЯ НОВОЙ ЭКОНОМИКИ



Современные, новые сектора экономики отличаются сетевым характером предоставления услуг. Сотовая связь, интернет, кабельное ТВ обслуживают колоссальное количество абонентов при относительно невысоких суммах регулярных платежей. Речь идет о десятках и сотнях миллионов клиентов, каждый из которых во многих случаях платит лишь по \$5–10 ежемесячно.

Так, например, средний доход на одного абонента (ARPU) в мобильной связи в России составляет более \$7. Средняя сумма платежа через систему «КиберПлат» (CyberPlat®) — \$8,5. В Москве средняя сумма платежа — выше \$12, в регионах России эта сумма составляет \$3, в Казахстане — \$5,9, а в Индии — \$2,1.

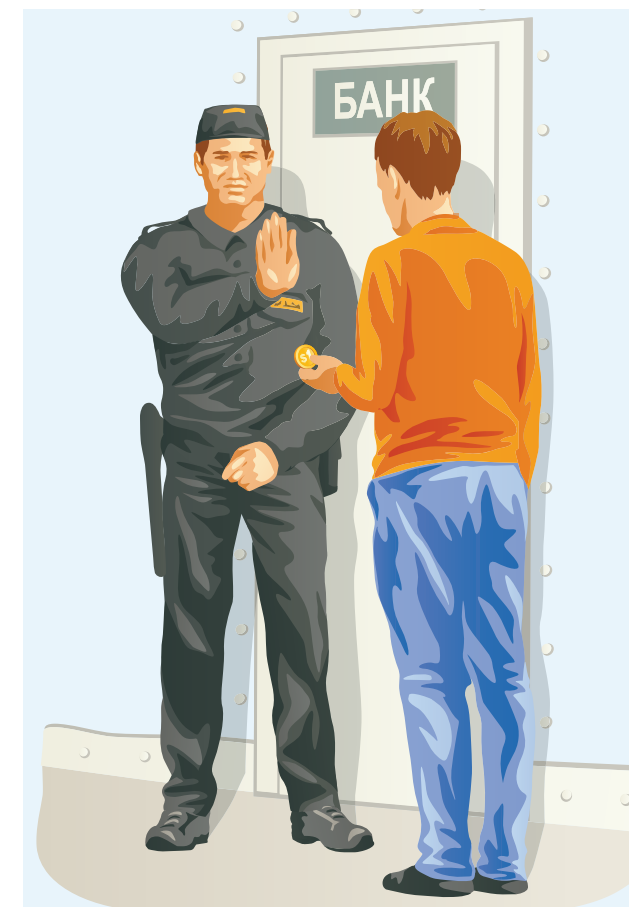
СОВРЕМЕННАЯ БАНКОВСКАЯ СИСТЕМА И ТРЕБОВАНИЯ НОВОЙ ЭКОНОМИКИ

Когда клиент сотового оператора пополняет в филиале обычного банка (в России около 30,7 тысяч банковских подразделений на более 146 миллионов жителей) свой абонентский счёт на \$5, себестоимость такой операции для банка, как показано выше, составляет примерно \$1. С учётом банковской маржи (ведь банк не может работать бесплатно) с клиента будет удержано около \$1,5, что составит примерно 30% от суммы платежа. Очевидно, такой размер комиссии будет неприемлем для клиента.

Этим и определяется необходимость формирования новой, более эффективной финансовой инфраструктуры для проведения большого количества сравнительно небольших по сумме платежей. Естественной базой такой новой инфраструктуры стали предприятия розничной торговли. Небольшие платежи легко может принимать кассир в магазине, чья зарплата существенно ниже, чем средняя зарплата банковского работника.

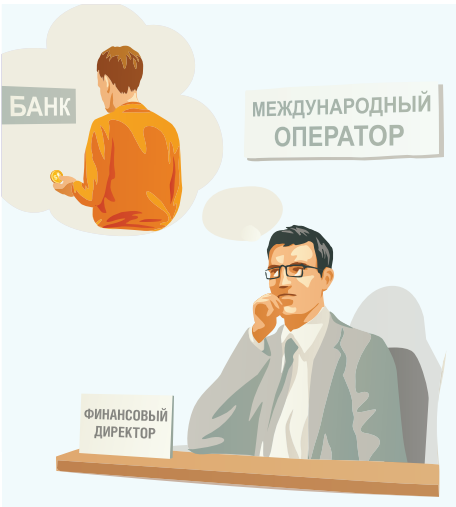
Кроме того, магазины не нуждаются в бронированных стенах, сейфах-хранилищах и сверхнадёжных системах охраны (для платежей в \$3–5 они просто не нужны). Соответственно, себестоимость приёма платежей в ритейле существенно ниже, чем в банках.

Понятно, что небольшие по суммам платежи не могут проводиться в большом количестве без создания новой финансовой инфраструктуры. Это означает, что без неё развитие новой экономики серьёзно затруднено — бизнес не имеет каналов сбора денег за свои услуги, а люди ограничены в пользовании современными цифровыми услугами. Отсутствие новой финансовой инфраструктуры является одной из причин классового разделения общества по признаку доступа к использованию современных сервисов и услуг, которое принято называть «цифровым неравенством» (Digital Divide).



НЕОБХОДИМОСТЬ МЕНЕЕ ЗАТРАТНОЙ ФИНАНСОВОЙ ИНФРАСТРУКТУРЫ

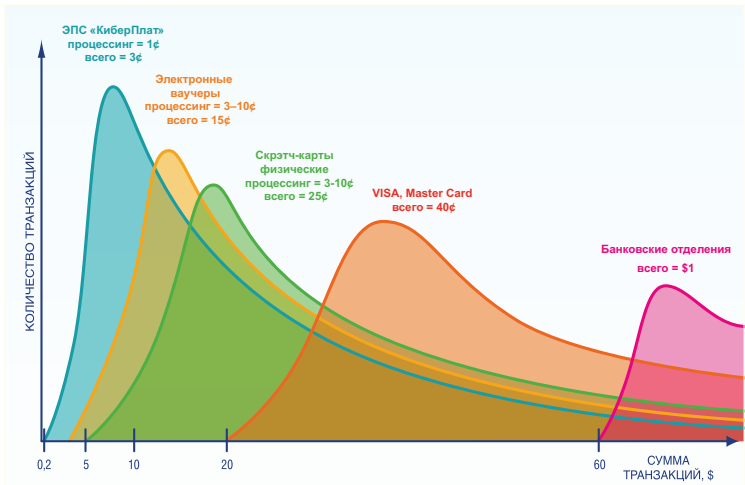
Совершенно очевидно, что для развития новой экономики необходима новая финансовая инфраструктура. Это не означает, что эта инфраструктура заменит собой уже существующую — она дополнит её и займёт собственную нишу. Можно предположить, что эта ниша — для сумм платежей, не превышающих \$50–100. Очевидно и то, что без новой финансовой инфраструктуры новая экономика не будет развиваться по-настоящему динамично, не будет охватывать широкие слои населения. Причина в том, что, как уже говорилось выше, новую экономику в основном представляют бизнесы с показателем ARPU (среднего дохода в месяц в расчёте на одного абонента), равным \$3–5.



ПЛАТЁЖНЫЕ ТЕХНОЛОГИИ «КИБЕРПЛАТ» (CYBERPLAT®) ВНЕ КОНКУРЕНЦИИ

Анализ представленных на рынке платёжных технологий показывает, что себестоимость платежей через систему «КиберПлат» (CyberPlat®) настолько мала (см. рисунок ниже), что делает выгодной организацию приёма платежей даже при минимальных суммах, не превышающих в среднем \$5. При этом может быть установлен такой уровень комиссионных сборов, который устраивает как,

к примеру, торговое предприятие, которое организует приём платежей по технологии «КиберПлат» (CyberPlat®), так и клиента, который не готов к 10–30%-ной комиссии (выше показано, что размер комиссии при приёме микроплатежей в банке может при минимальном уровне рентабельности доходить до 30%).

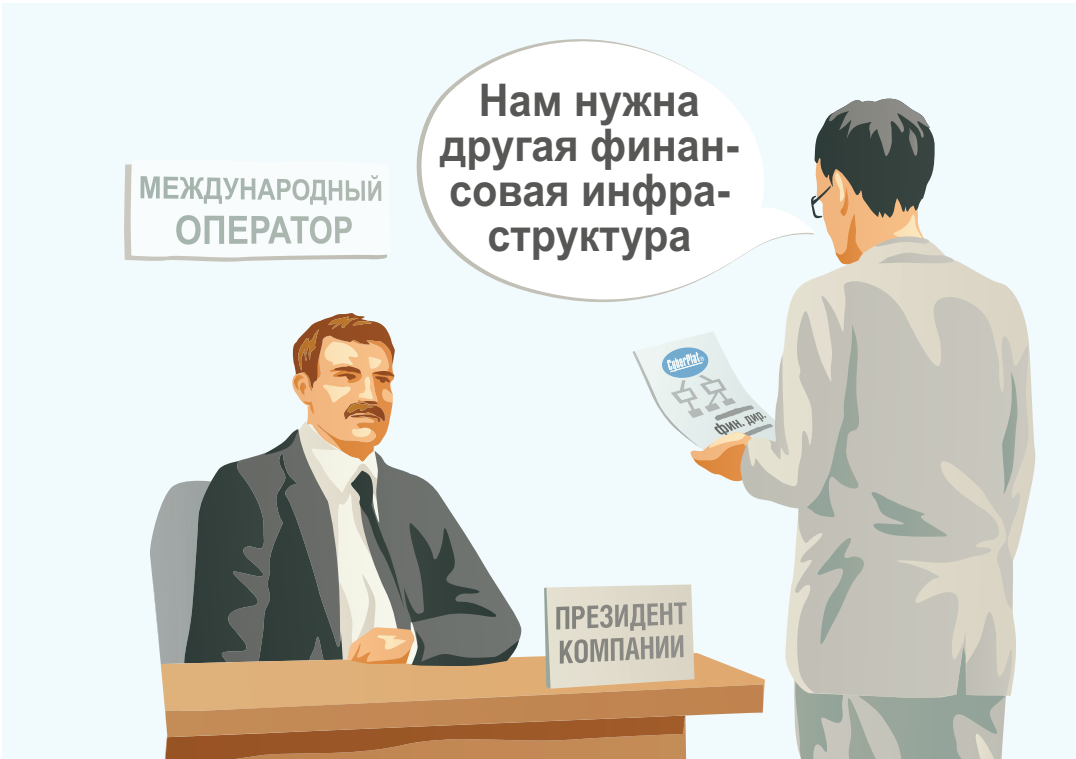


НЕВОЗМОЖНОСТЬ УДОВЛЕТВОРИТЬ НЕКОТОРЫЕ ТРЕБОВАНИЯ БЕЗ НИЗКОЗАТРАТНОЙ ФИНАНСОВОЙ ИНФРАСТРУКТУРЫ

На рынке сегодня широко представлены и динамично развиваются такие сервисы, как, к примеру, iTunes, предлагающие пользователям контент и продукты по относительно невысоким ценам — часто менее \$1. Сегодня в сети интернет вполне можно легально скачать и использовать хиты известных исполнителей по цене \$0,5, \$0,25 и даже меньше. Понятно, что такой бизнес не может развиваться без соответствующей системы приёма денег.

Это относится и к другим видам услуг по продаже интеллектуального контента, причем не только в сфере развлечений, — это доступ и к Google Earth, и к платным справочным сервисам и т.п. К примеру, система LexisNexis предоставляет клиентам доступ к миллионам документов и записям более чем из 45 тысяч правовых, новостных и бизнес-источников. Сервис доступен за абонентскую плату (примерно \$50 в месяц). Используя предлагаемые нами технологии, можно заплатить \$1, найти то, что нужно, и отключиться от интернет-сервиса.

Такие технологии микроплатежей, безусловно, способны придать серьезный импульс развитию новой экономики.



ЗАТРАТЫ НА ПРОИЗВОДСТВО СКРЕТЧ-КАРТ И ИНФРАСТРУКТУРУ ИХ РАСПРОСТРАНЕНИЯ

Инфраструктура микроплатежей является действительно значимой для провайдеров услуг. Она позволяет охватить все слои общества, в отличие от метода оплаты «по факту» (post paid), который предоставляет возможность работать только с теми пользователями, у кого есть банковский счёт, и только в тех странах, где разрешено прямое дебетовое списание со счёта.

Специально для клиентов со средним уровнем доходов телекоммуникационная индустрия создала такой финансовый продукт, как карта экспресс-оплаты (скретч-карта). Выпуск карт экспресс-оплаты достаточно затратен — производство каждой из них обходится, как минимум, в \$0,2. Однако скретч-карты позволяют охватить тот сегмент рынка, где платежи составляют от \$5 до \$25. Эти платежи нерентабельны, если их проводить через банки.

Выпускать же скретч-карты номиналом менее \$5 попросту невыгодно, о чем свидетельствуют данные приведённой ниже таблицы.

СТОИМОСТЬ ПРОИЗВОДСТВА И РАСПРОСТРАНЕНИЯ СКРЕТЧ-КАРТ (% ОТ НОМИНАЛА)

Номинал	Стоимость производства	Комиссия дилера	Общие издержки
\$15	1 %	7 %	8 %
\$10	2 %	9 %	11 %
\$6	4 %	10 %	14 %
\$4	5 %	12 %	17 %
\$3	10 %	18 %	28 %
\$2	20 %	25 %	45 %
\$1	30 %	30 %	60 %

Таким образом, понятно, что выпускать скретч-карты номиналом менее \$5 невозможно, поскольку их себестоимость начинает превышать неприемлемые 30–40 %.

МЕЛКИЕ ПЛАТЕЖИ

Для охвата самых малоимущих слоёв населения (дети, трудовые мигранты, люди с невысоким уровнем доходов, средние слои населения стран Африки и Азии) принципиально важно использовать недорогие методы осуществления платежей.

У людей с низким доходом обычно не бывает с собой более \$2



НАДЁЖНАЯ ТЕХНОЛОГИЯ

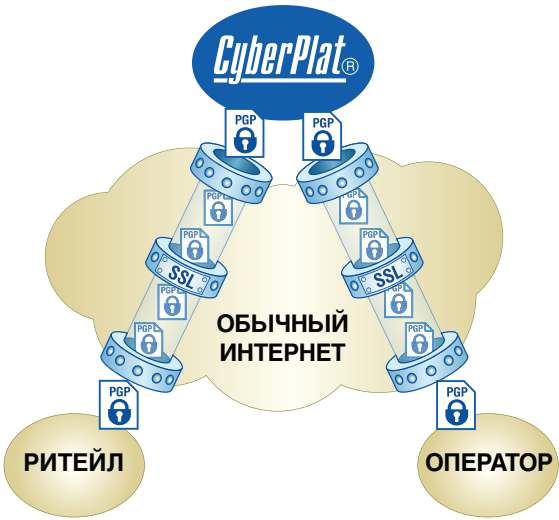
Принципиально важно, что предлагаемые «КиберПлат» (CyberPlat®) недорогие методы осуществления платежей обладают высочайшей надёжностью.

Каждый провайдер и все агенты системы электронных платежей подключены к процессингу «КиберПлат» (CyberPlat®) через интернет — это может быть выделенная линия, связь по телефонному номеру (dial-up) или обычная пакетная система передачи данных GPRS.

При каждой такой транзакции устанавливается SSL-соединение (протокол безопасных соединений), при помощи которого передаются файлы размером в 1 килобайт, закодированные и заверенные электронной цифровой подписью.

Поскольку размер файла очень мал, это позволяет использовать любой вид интернет-соединения — даже очень слабое соединение.

Надёжность таких транзакций высока (для шифрования используется 2048-битовый ключ) и более чем достаточна для платежей размером в \$5. За более 20 лет работы системы «КиберПлат» (CyberPlat®) не произошло ни одного случая взлома системы. Опыт показал, что ни теоретически, ни практически такую систему взломать невозможно.



ПОЧЕМУ ЭТО ПОПУЛЯРНО

100 SMS
бесплатно!



ОХВАТ МОБИЛЬНОЙ СВЯЗЬЮ

Почему бизнес «КиберПлат» (CyberPlat®) так быстро развивался, например, в России? Потому что он обеспечил фактически более чем 100%-ный охват населения мобильной связью. Сегодня даже ребёнок в малоимущей российской семье пользуется мобильным телефоном. Данные авторитетных международных исследований говорят о факте роста числа действующих SIM-карт в России до 250 миллионов на более чем 146 миллионов жителей. Эксперты при подсчёте учитывают людей, которые используют несколько мобильных телефонов, а также определённое количество «молчащих» SIM-карт. В действительности коэффициент использования мобильной связи в России составляет около 90%. Это доказывает тот

факт, что даже каждый ребёнок в России пользуется мобильной связью.

Это возможно только потому, что ребёнок способен переводить свои пусть даже очень скромные карманные деньги на счёт мобильного телефона.

После начала работы системы несколько миллионов малообеспеченных юных абонентов начали пользоваться услугами «КиберПлат» (CyberPlat®), поскольку они вполне могут себе позволить потратить 150–200 рублей в месяц на оплату мобильной связи. Некоторые региональные операторы сотовой связи предоставляют возможность в своих тарифных планах отправлять до 100 SMS-сообщений бесплатно — этим активно и пользуются дети, которые реже применяют голосовую связь, но активно общаются в SMS-формате.

РОСТ ТРАФИКА СО СТОРОНЫ РОДИТЕЛЕЙ

Дети генерируют входящий трафик от их родителей. Именно по этой причине они являются важной категорией клиентов для операторов мобильной связи. Действительно, регулярные звонки родителей детям («Где ты?», «Когда ты пришёл домой из школы?», «Ты покушал?», «Сделал ли ты уроки?» и т.п.) приводят к серьёзному росту голосового трафика со стороны родителей и, соответственно, увеличивают доходы операторов сотовой связи.



Средняя выручка за месяц в расчёте
на одного абонента (ARPU)

О КОМПАНИИ

ОБЩИЕ СВЕДЕНИЯ



В 1997 году на базе отдела электронной коммерции банка «Платина» была создана интегрированная универсальная мультибанковская система платежей «КиберПлат» (CyberPlat®). Она разрабатывалась с целью информационно-технологического обеспечения безналичных расчётов для электронной коммерции всего спектра финансовых услуг — от микроплатежей до межбанковских расчётов. Как отдельная компания «КиберПлат» (CyberPlat®) был выделен в 2000 году.

«КиберПлат» (CyberPlat®) является исторически первой российской системой электронных платежей — 18 марта 1998 года была совершена первая транзакция в пользу компании «Гарант-Парк», а 12 августа 1998 года осуществлен первый онлайн-платёж через интернет в пользу оператора сотовой связи «Билайн».

За более чем 20 лет работы на рынке компанией накоплен огромный опыт по организации приёма платежей в торговых и сервисных сетях. К концу 2018 года через систему принимались платежи в пользу более 8 тысяч поставщиков услуг, включая компании сотовой и фиксированной связи, кабельного ТВ, провайдеров проводного и мобильного интернета, систем охранной сигнализации, предприятий ЖКХ и энергосбытовых компаний практически во всех регионах Российской Федерации. Через систему «КиберПлат» (CyberPlat®) можно оплачивать авиационные и железнодорожные билеты, погашать банковские кредиты и осуществлять денежные переводы, а также вносить платежи в пользу государства: оплачивать налоги и сборы, штрафы ГИБДД, разрешения на работу и др.

Благодаря постоянной модернизации технологической платформы система электронных платежей «КиберПлат» (CyberPlat®) способна на сегодняшний день проводить более 1400 финансовых транзакций в секунду — этот рекордный для России показатель обеспечивает 15-кратный запас по отношению к максимальным пиковым нагрузкам на систему.

Подобная производительность дополняется абсолютной защищённостью финансовых транзакций. В рамках одной транзакции в системе совершается до 16 операций (проводок), заверенных электронной подписью и осуществляющихся с использованием защищённых способов передачи данных по каналам интернета. Такая технология обеспечивает абсолютную безопасность совершаемых финансовых транзакций и минимизирует количество ошибочных платежей. В системе «КиберПлат» (CyberPlat®) не произошло ни одного случая взлома информационной системы и проведения незаконных транзакций.

По критериям надёжности и бесперебойности система электронных платежей «КиберПлат» (CyberPlat®) также не имеет себе равных на российском рынке — показатель отказоустойчивости системы превосходит аналогичный показатель ближайших конкурентов в несколько раз.

Партнёрами по организации приёма платежей, оценившими преимущества системы «КиберПлат» (CyberPlat®), являются все крупные игроки рынка телекоммуникаций, крупнейшие российские банки, включая «Сбербанк России», ВТБ, «Почта Банк»,

«Альфа-банк», «Россельхозбанк», «Росбанк», «Юникредит», «Россия», «Банк Русский Стандарт» и пр., федеральные торговые сети «Эльдорадо», «Евросеть» и т.д., АО «Казпочта», государственные структуры, энергосбытовые и транспортные компании, предприятия ЖКХ и многие другие.

Система «КиберПлат» (CyberPlat®) выполняет важнейшую для государства функцию обеспечения большого объёма платежей со стороны населения в пользу различных поставщиков товаров и услуг, что способствует активному развитию новых секторов экономики, основанных на предоставлении современных услуг в сферах телекоммуникаций, банковского и страхового дела, розничной торговли. В последнее время значительно возрастает доля платежей за коммунальные услуги и в адрес государственных структур (налоги, пошлины, сборы, штрафы). Система электронных платежей «КиберПлат» (CyberPlat®) была выбрана партнёром Федерального казначейства и Федеральной налоговой службы и принимала участие в пилотных проектах по разработке новых механизмов финансового взаимодействия граждан и государственных структур.

НАГРАДЫ ПАРТНЁРОВ

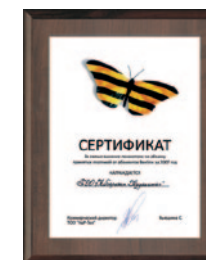
Устойчивый рост оборота и качества услуг «КиберПлат» (CyberPlat®) делает систему электронных платежей лидером в своём секторе рынка. Признанием этого являются десятки наград и дипломов, полученных от партнёров компании. Так, например, компания МТС по результатам комплексного мониторинга своих крупнейших партнёров по приёму платежей признала «КиберПлат» (CyberPlat®) самой надёжной процессинговой системой. Деловая активность компании «КиберПлат» (CyberPlat®) также подтверждена наградами других компаний.



Билайн



Билайн



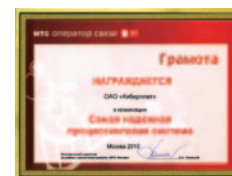
Билайн



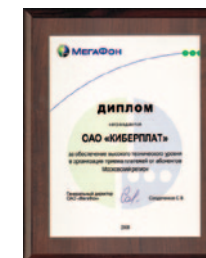
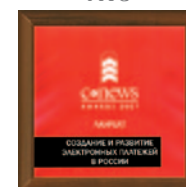
МегаФон



Билайн



МТС



МегаФон



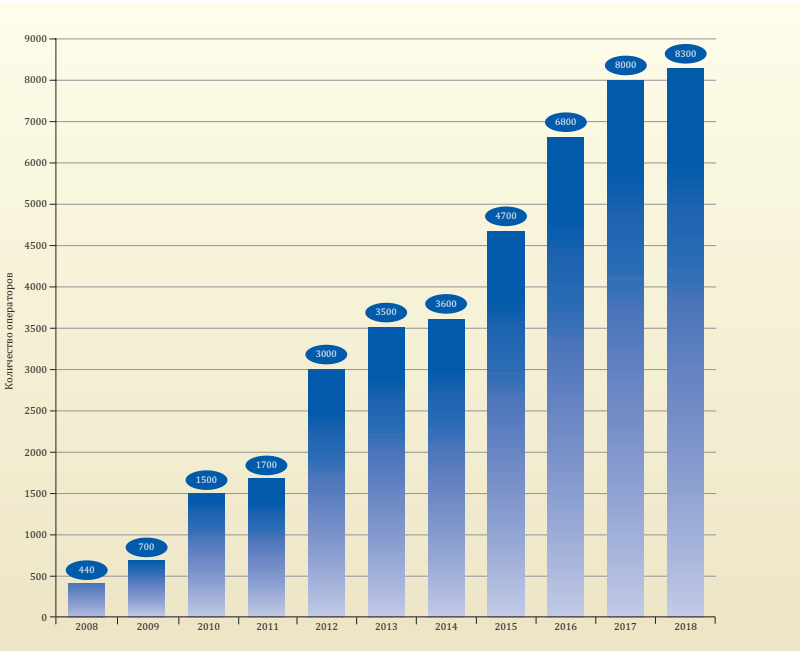
МТС

ОСНОВНЫЕ ПОКАЗАТЕЛИ

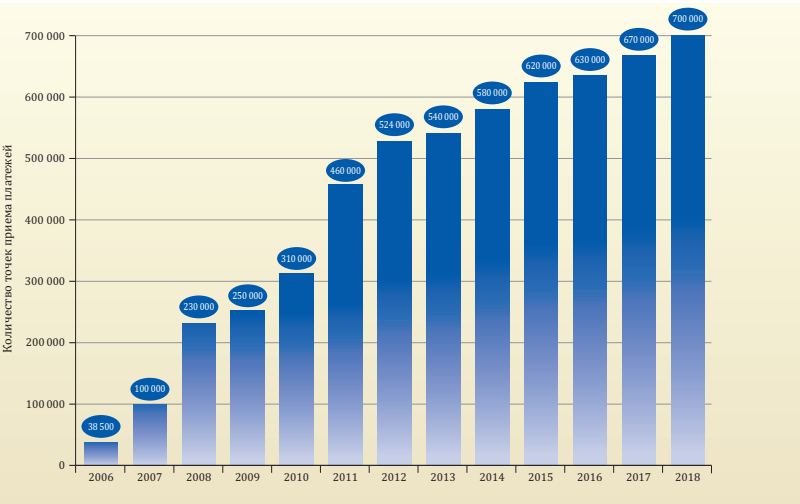
В 2018 году «КиберПлат» (CyberPlat®), как и в предыдущие годы, показала устойчивую динамику бизнеса. Общее число пунктов приёма платежей превысило 1 480 000, из которых более 700 тысяч находятся в России и странах СНГ, а остальные — в крупнейших городах многих стран мира.

Общее количество точек приёма платежей системы «КиберПлат» (CyberPlat®) в России и СНГ в настоящее время более чем в 20 раз превышает размеры всей российской банковской системы (количество банковских учреждений со всеми филиалами, отделениями и даже передвижными кассами в РФ составляло на 1 января 2019 года около 31 000).

По состоянию на конец 2018 года более 250 банков являются участниками системы.



Динамика количества провайдеров



Динамика количества точек приёма платежей в России странах СНГ

ОТЗЫВЫ ПАРТНЁРОВ О СИСТЕМЕ «КИБЕРПЛАТ» (CYBERPLAT®)



Самохвалов Александр Владимирович,
Председатель Правления
АО «Банк Русский Стандарт»:

Наш банк — участник системы электронных платежей «КиберПлат» (CyberPlat®), и должен сказать, что за всё время нашего сотрудничества мы ни разу об этом не пожалели. Специалистами «КиберПлат» (CyberPlat®) разработан целый спектр прекрасных продуктов для банков, многие из них нами активно используются — мы принимаем платежи через систему «КиберПлат» (CyberPlat®), интегрировали эту возможность и в нашу систему интернет-банкинга для клиентов. Использование технологий «КиберПлат» (CyberPlat®) позволяет совершенствовать наш бизнес, делать его более эффективным.

ЕВРОСЕТЬ

Гуськова Оксана Александровна,
СЕО Объединенной компании Связной | Евросеть:

«КиберПлат» (CyberPlat®) была пионером рынка приёма платежей и на протяжении многих лет делала так, что российский потребитель мог заплатить за самые разные услуги самым удобным способом. «КиберПлат» (CyberPlat®) — наш давний и надёжный партнёр.



Галушко Евгений Павлович,
Генеральный директор розничной сети МТС:

Система «КиберПлат» (CyberPlat®) внесла существенный вклад в развитие сервисов по приёму платежей в России, благодаря которым в том числе мобильная связь в стране стала массовой и доступной услугой. Компания постоянно ищет новые пути развития, совершенствуя уже запущенные сервисы, и мы ценим продуктивное сотрудничество с «КиберПлат» (CyberPlat®) — это один из каналов пополнения счёта для наших пользователей. «КиберПлат» неоднократно становилась победителем тендеров МТС в различных регионах, мы также давно сотрудничаем с «КиберПлат» (CyberPlat®) по приёму платежей через кассы салонов розницы МТС.



Поколотный Даниил Сергеевич,
Директор по телекоммуникационным
и финансовым услугам ГК «Связной»:

Широкий спектр клиентских услуг, представленных в сети «Связной», стал одним из ключевых драйверов роста бизнеса нашей компании.

Учитывая популярность финансовых услуг среди клиентов и наше стремление предоставлять сервис самого высокого уровня, мы сотрудничаем только с самыми надёжными и эффективными партнёрами, каким, несомненно, является и система электронных платежей «КиберПлат» (CyberPlat®). Вместе с «КиберПлат» (CyberPlat®) мы уже реализовали такие услуги, как оплата коммунальных платежей, штрафов ГИБДД, платежи в пользу энергосбытовых компаний, возможность пополнения карт. Уверен, что в дальнейшем список наших совместных проектов будет расширяться и мы сможем предложить клиентам нашей сети ещё больше дополнительных возможностей.

КАК РАБОТАЕТ «КИБЕРПЛАТ» (CYBERPLAT®)

СХЕМА ОРГАНИЗАЦИИ БИЗНЕСА «КИБЕРПЛАТ» (CYBERPLAT®)



ПАРТНЁРЫ КОМПАНИИ

Вопрос оптимизации издержек при сборе выручки за свои услуги с ростом клиентской базы становится для поставщиков услуг всё более актуальным. Система «КиберПлат» (CyberPlat®) позволяет сделать более эффективным процесс сбора выручки, поэтому количество организаций, использующих «КиберПлат» (CyberPlat®), динамично растёт в течение всего периода работы компании на рынке.

Сегодня система электронных платежей «КиберПлат» (CyberPlat®) интегрирует платёжные шлюзы к крупнейшим провайдерам услуг, включая ведущих операторов мобильной и фиксированной связи, операторов спутникового и кабельного телевидения, организаций жилищно-коммунального комплекса, энерго- и газосбытовые компании и многие другие.

Ниже представлены крупнейшие в своих секторах операторы, к которым разработаны прямые платёжные шлюзы. Кроме того, в системе «КиберПлат» (CyberPlat®) представлены все значимые операторы услуг всех регионов Российской Федерации (включая региональные жилищно-коммунальные, газо- и энергосбытовые компании), платежи в пользу которых проводятся через шлюз «Банковский провайдер».

НЕКОТОРЫЕ КРУПНЕЙШИЕ ОПЕРАТОРЫ И ПРОВАЙДЕРЫ УСЛУГ

Сотовая связь

	МТС Общероссийский оператор
	МегаФон Общероссийский оператор
	Билайн Общероссийский оператор
	Tele2 Общероссийский оператор
	Мотив Екатеринбург и Свердловская область

Фиксированная связь



Ростелеком
Общероссийский оператор



МГТС
Москва



Транстелеком
Общероссийский оператор



Сумма Телеком
в Санкт-Петербурге, Нижнем Новгороде,
Туле, Твери, Орле, Липецке, Воронеже,
Ростове-на-Дону, Краснодаре и Махачкале,
Дербенте, Каспийске, Кизилюрте

Телевидение и интернет



НТВ-Плюс
Общероссийский оператор



Триколор-ТВ
Общероссийский оператор



АКАДО
Москва



Yota
Москва



Дом.ру



Орион Экспресс

Коммунальные платежи



Газпром Межрегионгаз



Мособлгаз



ТНС Энерго



Мосэнергосбыт
Москва



МособлЕИРЦ



АО «ЕИРЦ ЛО»



Дальэнергосбыт



**Свердловская
энергогазовая
компания**



Якутскэнерго



Тюменская энергосбытовая компания



**Екатеринбургская
электросетевая компания**

Охранные системы



Цезарь Сателлит
Спутниковая охранная система



Автолокатор
Спутниковая
противоугонная система



Cobra Connex
Спутниковая охранно-поисковая система



Гольфстрим
Спутниковая охранная система

Авиабилеты



Озон-Трэвел
Бронирование авиабилетов



Туроператор «Интурист»



UFS
Бронирование авиа-
и железнодорожных билетов



Билет-Он-Лайн
Продажа авиа- и железнодорожных билетов



Туроператор «Дельфин»

Товары (прямые продажи)



Avon



Oriflame



Faberlic



Zepter

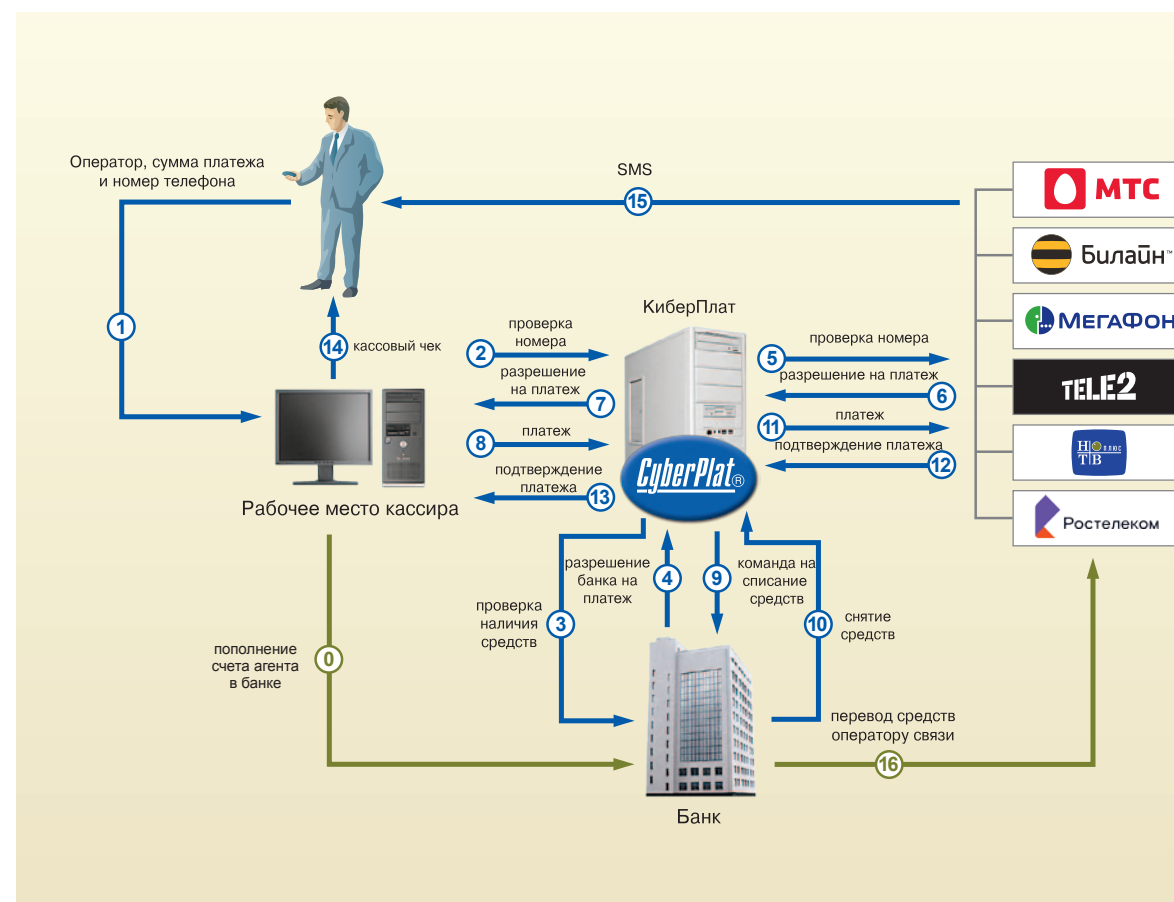
Ознакомиться с полным списком провайдеров услуг можно
на сайте компании: <http://www.cyberplat.ru/about/providers>

ТЕХНОЛОГИЯ «КИБЕРПЛАТ» (CYBERPLAT®): СХЕМА ТИПОВОГО РЕШЕНИЯ НА ПРИМЕРЕ DOMESTIC TOP-UP

«КиберПлат» (CyberPlat®) осуществляет организацию приёма платежей за услуги операторов в режиме онлайн.

Компания-агент, принимающая деньги у абонента, гарантирует мгновенное пополнение лицевого счёта абонента в биллинговой системе оператора. Для проведения операций используется принципиально новая платёжная схема B2B(4C), объединяющая возможности существующих схем межкорпоративных интернет-расчётов и электронных платежей физических лиц.

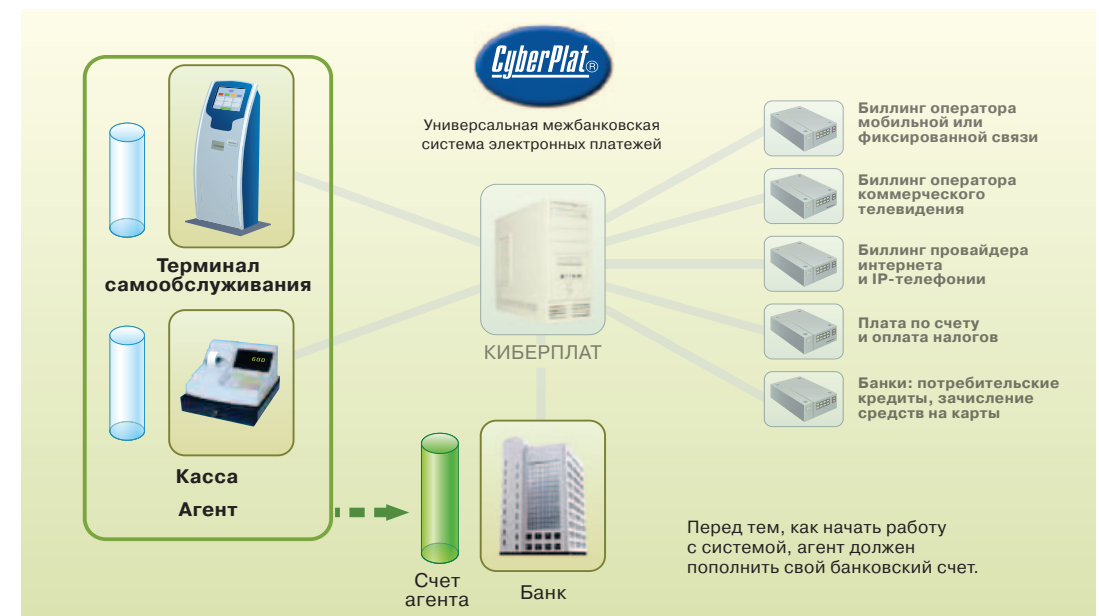
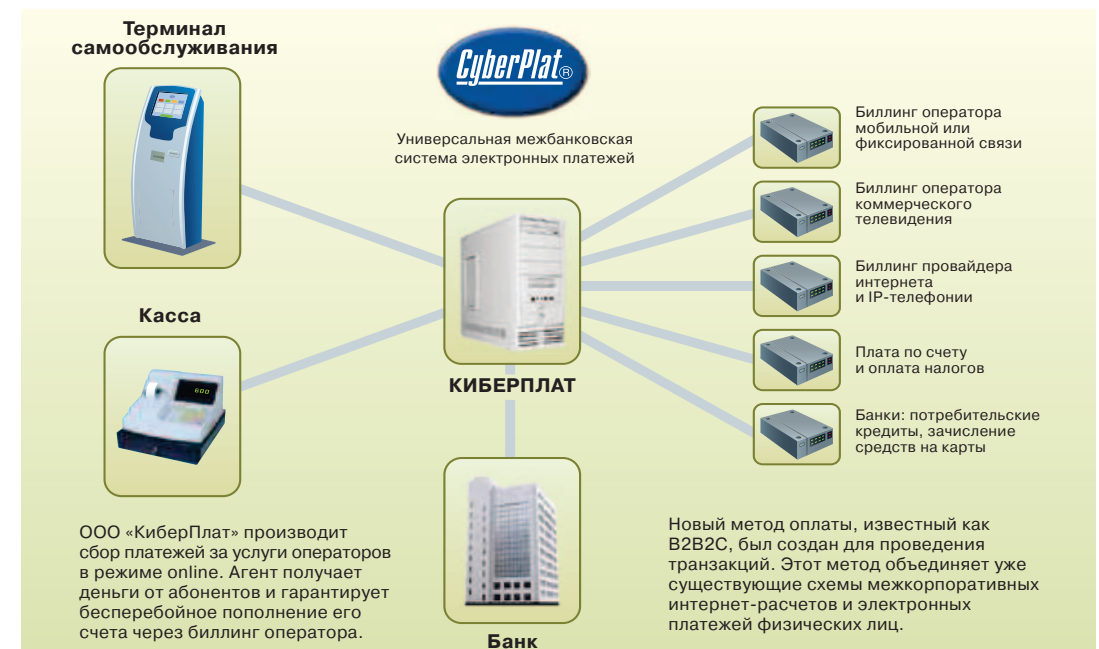
Детально процесс выглядит следующим образом:

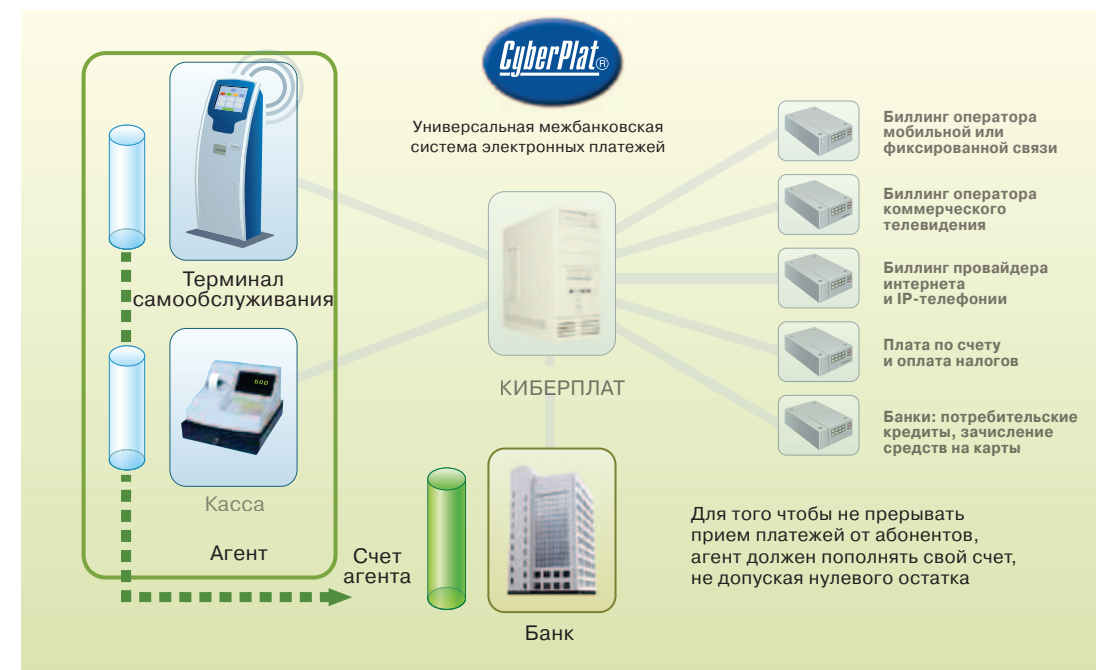


0. Агент переводит в расчётный банк системы электронных платежей «КиберПлат» (CyberPlat®) сумму, обеспечивающую проведение платежей.
1. Абонент при оплате товаров на кассе сообщает кассиру о намерении внести желаемую сумму на номер своего мобильного телефона (например, компании МТС, Билайн, МегаФон, Tele2, другого оператора сотовой связи, а также провайдера телекоммуникационных услуг). Кассир вводит номер телефона и сумму и нажимает кнопку «Оплатить».
2. Персональный компьютер или любое другое программно-аппаратное устройство (POS-терминал, кассовый аппарат) пункта приёма платежей по защищённому интернет-протоколу SSL пересылает запрос на проверку телефонного номера на сервер компании ООО «КИБЕРПЛАТ». При этом запрос заверяется электронной подписью (ЭП).
3. С сервера компании ООО «КИБЕРПЛАТ» запрос отправляется на сервер расчётного банка системы «КиберПлат» (CyberPlat®) с целью проверки наличия необходимых для осуществления платежа средств на счёте агента. Использование защищённых интернет-протоколов SSL и электронной цифровой подписи гарантирует абсолютную безопасность.
4. Сервер банка отправляет на сервер «КиберПлат» (CyberPlat®) ответ о наличии либо недостатке средств на счёте агента.
5. При положительном ответе банка запрос на проверку номера, подписанный ЭП ООО «КИБЕРПЛАТ», с сервера компании по SSL-протоколу отправляется в биллинговую систему оператора.
6. Биллинг оператора проверяет наличие данного телефонного номера и отправляет разрешение на платёж на сервер «КиберПлат» (CyberPlat®).
7. Сервер «КиберПлат» (CyberPlat®) отправляет разрешение на платёж на рабочее место операциониста в пункт приёма платежа агента.
8. Операционист пункта приёма платежей принимает от абонента денежные средства в размере суммы платежа и нажимает кнопку «Подтвердить платёж». Платёж отправляется на сервер «КиберПлат» (CyberPlat®).
9. Сервер «КиберПлат» (CyberPlat®) отправляет на сервер расчётного банка команду (электронный платёжный документ) на списание внесённой в кассу суммы со счёта агента.
10. На сервер «КиберПлат» (CyberPlat®) отправляется подтверждение о снятии денежной суммы.
11. Платёж с сервера «КиберПлат» (CyberPlat®) отправляется в биллинг оператора, после чего происходит пополнение лицевого счёта абонента в биллинге оператора.
- 12, 13. Биллинг оператора отправляет подтверждение о получении средств, которое приходит на рабочее место кассира пункта приёма платежа агента, что видят и кассир, и покупатель.
14. Кассовый аппарат печатает и выдаёт абоненту фискальный чек со всеми параметрами совершенного платежа (оператор связи, дата, сумма, номер телефона).
15. Биллинг оператора отправляет SMS-сообщение на сотовый телефон абонента с подтверждением пополнения лицевого счёта.
16. Денежные средства со счёта компании-агента в расчётном банке переводятся на счёт оператора.

Используемая при этом технология электронного документооборота CyberFT характеризуется высочайшей скоростью (время электронного платежа через систему составляет не более двух секунд при условии хорошего канала выхода в интернет у дилера) и безопасностью, гарантируемой обязательным использованием электронных цифровых подписей сторон.

МОДЕЛЬ РАБОТЫ «КИБЕРПЛАТ» (CYBERPLAT®)





Мультимедийная презентация модели работы системы «КиберПлат» (CyberPlat®) размещена на сайте :
https://www.cyberplat.ru/advantages/how_does_it_work/

БАНКИ — ПАРТНЁРЫ СИСТЕМЫ «КИБЕРПЛАТ» (CYBERPLAT®)

К концу 2018 года система электронных платежей «КиберПлат» (CyberPlat®) имела договорные отношения с более чем 250 банками. Многие банки сотрудничают с системой в качестве агентов, организуя приём платежей через систему «КиберПлат» (CyberPlat®) в своих офисах, банкоматах или в сетях банковских терминалов самообслуживания. Одновременно многие из них выступают и в качестве операторов, получателей платежей, используя «КиберПлат» (CyberPlat®) как эффективный канал погашения выданных физическим лицам кредитов и пополнения банковских, в том числе карточных, счетов.

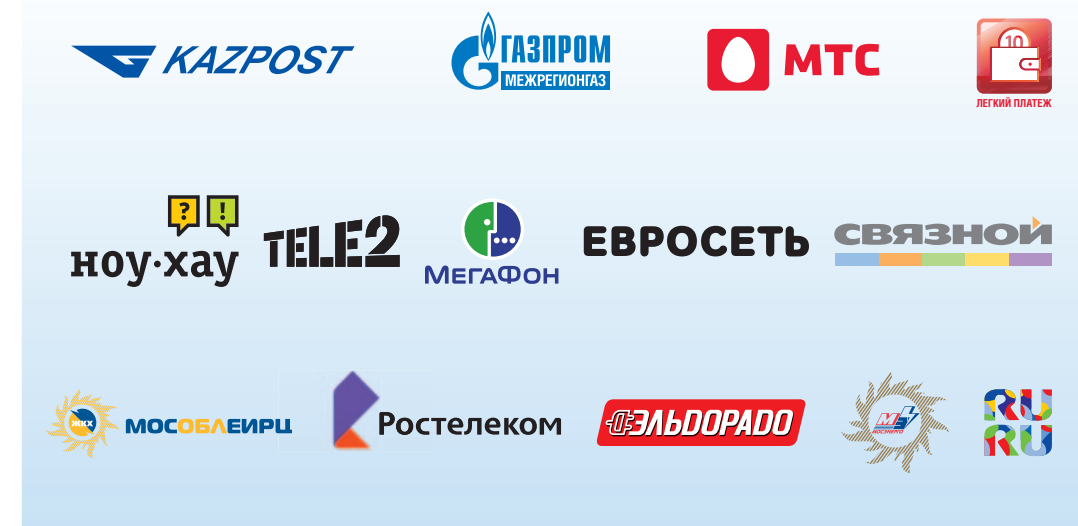
Многие банки в своей деятельности используют уникальный продукт, разработанный специалистами «КиберПлат» (CyberPlat®), — Интегратор систем денежных переводов (ИСДП), многократно повышающий эффективность в сфере бизнеса денежных переводов. Ниже приведены только некоторые крупнейшие банки-партнёры.



СЕТЬ ПРИЁМА ПЛАТЕЖЕЙ (КРУПНЕЙШИЕ РИТЕЙЛЕРЫ)

На сегодняшний день наиболее известными агентами компании ООО «КИБЕРПЛАТ» являются:

- федеральные сети салонов связи «Связной», «Евросеть», «Ной-Хау», монобрендовые сети салонов связи МТС, МегаФон, Tele2;
- АО «Казпочта»;
- отделения Мособлеирц, Леноблеирц;
- сети магазинов электроники «Эльдорадо»;
- сети платёжных терминалов «Элекснет», «ПлатёжКа»;
- «Россельхозбанк», «Альфа-Банк», Банк «Русский Стандарт», Банк «Россия», «СДМ-Банк», «Промсвязьбанк», Банк «Санкт-Петербург», «СМП Банк» и многие другие.



Основные сети приёма платежей

ГЕОГРАФИЯ БИЗНЕСА

«КИБЕРПЛАТ» (CYBERPLAT®)

Региональные представительства «КиберПлат» (CyberPlat®) успешно действуют в разных федеральных округах Российской Федерации и расположены в Самаре, Курске, Екатеринбурге, Ставрополе.

Компания «КиберПлат» (CyberPlat®) успешно развивает свой бизнес на территории стран СНГ — в Казахстане работает дочерняя компания системы электронных платежей.

«КиберПлат» (CyberPlat®) является исторически первой системой электронных платежей в Казахстане. Дочерняя компания в Казахстане — ТОО «КиберПлат-Казахстан» — зарегистрирована 15 сентября 2005 года. Первые платежи через систему были осуществлены в апреле 2006 года. В конце 2018 года в Казахстане насчитывалось уже более 20 тысяч точек приёма платежей, подключённых к системе «КиберПлат» (CyberPlat®), а региональные представители компании работают во всех крупнейших городах Казахстана: Алма-Ате, Астане, Актюбинске, Чимкенте, Усть-Каменогорске, Караганде, Павлодаре, Кустанае и Уральске.

На сегодняшний день партнёрами дочернего предприятия «КиберПлат» (CyberPlat®) в Казахстане являются крупнейшие банки, сотовые операторы, провайдеры услуг, терминальные сети и торговые предприятия Республики Казахстан.

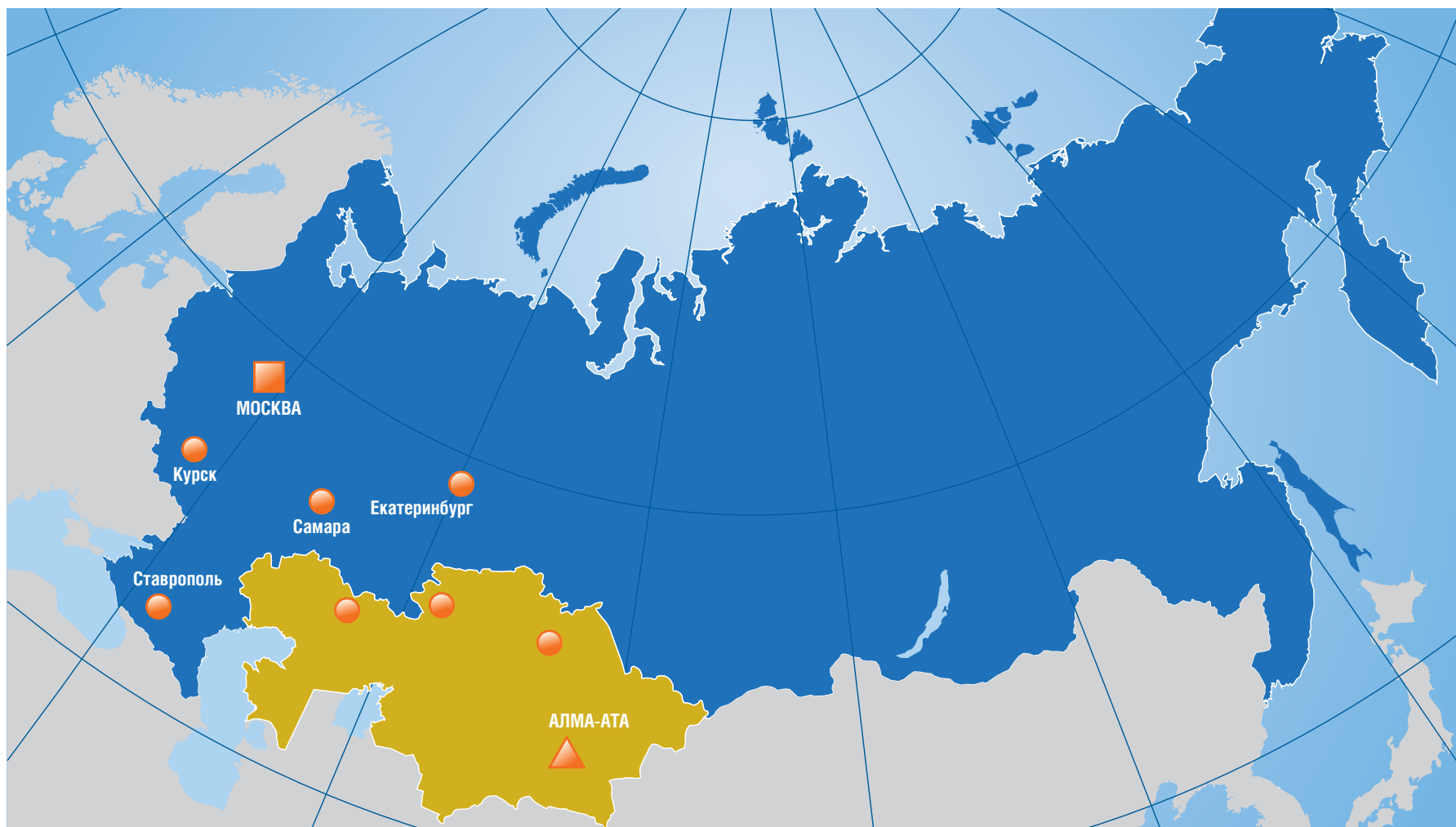
Один из самых крупных международных проектов «КиберПлат» (CyberPlat®) стартовал в 2009 году в Индии. Компании CyberPlat India, основанная в городе Мумбаи, развивалась стремительными темпами и несколько лет подряд демонстрировала ежегодный 100%-ный прирост, уверенно опережая конкурентов.

В настоящее время CyberPlat India является одним из лидеров национальной финтехиндустрии. Компания входит в ТОП-5 платёжных

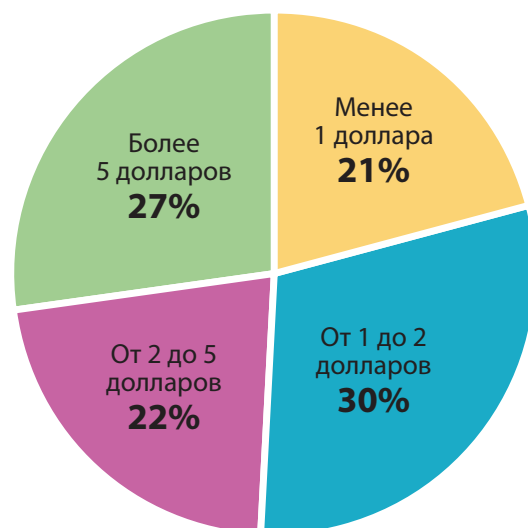
систем, работающих на одном из крупнейших рынков Азии, и занимает 1-е место по количеству пунктов приёма платежей в стране: на 1 января 2019 года их число превышало 760 тысяч. Ежегодно в системе осуществляется более 240 миллионов транзакций в пользу более 350 поставщиков услуг в Индии и за её рубежами, доступных в 600 партнёрских сетях.

CyberPlat India один из немногих среди платёжных агрегаторов Индии напрямую сотрудничает более чем с двумя десятками крупнейших провайдеров, предоставляющих услуги в сфере телекоммуникаций, спутникового ТВ и ЖКХ.

Сеть представительств «КиберПлат» (CyberPlat®) в странах СНГ



СОЦИАЛЬНАЯ МИССИЯ СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ «КИБЕРПЛАТ» (CYBERPLAT®)



Как свидетельствуют статистические данные, на конец 2018 года лишь около 28% платежей, проводимых через платёжную систему «КиберПлат» (CyberPlat®), превышает \$5. При этом платежи до \$1 занимают долю в 21%, от \$1 до \$2 — 30%, от \$2 до \$5 — 22%. Более 50% всех транзакций «КиберПлат» (CyberPlat®) составляют платежи до \$2, или примерно 117 рублей.

Приведенные данные свидетельствуют о том, что «КиберПлат» (CyberPlat®) обеспечивает возможность использования современных достижений высоких технологий для населения со средними и низкими

доходами. Прежде всего речь идет о мобильной связи и интернет-доступе. Ведь даже минимальный баланс позволяет абоненту оставаться на связи, посылать сообщения и делать срочные звонки.

Создаваемые системой «КиберПлат» (CyberPlat®) условия для использования современных коммуникационных технологий самыми широкими слоями населения играют решающую роль в преодолении проблемы так называемого цифрового неравенства в России. Статистические данные преобладания небольших платежей и общее количество транзакций, проходящих через систему, наглядно демонстрируют, что работа системы «КиберПлат» (CyberPlat®) способствует росту уровня проникновения мобильной связи в России.

К примеру, если у клиента закончились средства на счёте и недостаточно денег, чтобы купить скретч-карту за 100 рублей (минимальный номинал), то он может пополнить свой баланс в любом пункте приёма платежей.

Любой абонент, располагая суммой всего лишь в 10–20 рублей, может пополнить свой счёт и пользоваться SMS-услугами, а также принимать входящие звонки.

Удобно и то, что пунктами приёма платежей являются наиболее часто посещаемые места — магазины, аптеки, почтовые отделения, салоны связи, платёжные терминалы, автозаправки. При этом благодаря транзакции в реальном времени сумма платежа оказывается на балансе абонента мгновенно.

Таким образом, возможность вносить на счёт малые суммы предоставляет доступ к мобильной связи лицам с невысокими доходами, в частности детям, студентам и пенсионерам, что выполняет важную социальную миссию сокращения цифрового неравенства.

ПРЕИМУЩЕСТВА ТЕХНОЛОГИЙ «КИБЕРПЛАТ» (CYBERPLAT®)

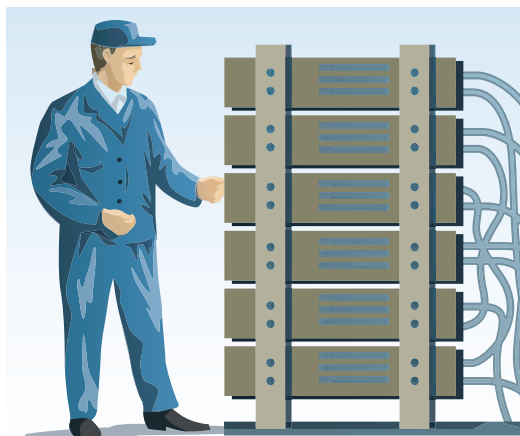
ОПЫТ И КВАЛИФИЦИРОВАННЫЕ КАДРЫ



Важным преимуществом системы «КиберПлат» (CyberPlat®) является организационно-технический и кадровый потенциал, накопленный компанией за 20 лет работы на рынке онлайн-платежей, который во многом и был создан благодаря усилиям специалистов и руководства системы.



Сегодня в компании работает более 200 специалистов, располагающих уникальными знаниями и навыками в своей сфере, — системные аналитики, программисты, специалисты в области финансов и банковского дела, в сфере автоматизации этих отраслей, юристы со знанием всех аспектов законодательного регулирования рынка моментальных платежей.



БЕЗОПАСНОСТЬ И ЗАЩИЩЕННОСТЬ



«КиберПлат» (CyberPlat®) — система электронных платежей закрытого типа. Её принципиальное отличие от систем открытого типа в том, что все участники расчётов — плательщики (агенты, принимающие платежи от абонентов) и получатели — жёстко определены. Средства со счёта торговой точки могут быть переведены только на счёт оператора и зачислены на лицевой счёт абонента. Вывод средств из системы по желанию сотрудника пункта приёма платежей невозможен.

«КиберПлат» (CyberPlat®) является системой, работающей в реальном времени. Любая транзакция в системе занимает не более двух секунд. Подобная беспрецедентная производительность дополняется абсолютной защищённостью финансовых транзакций.

В рамках одной транзакции в системе совершается до 16 операций (проводок), заверенных электронной цифровой подписью. Используются защищённые способы передачи данных по каналам интернета, включающие проверку наличия номеров телефонов или лицевых счетов клиентов в биллинговых системах провайдеров услуг, идентификацию и авторизацию точек приёма платежей и другие операции. Такая технология обеспечивает абсолютную безопасность совершаемых финансовых транзакций и минимизирует количество ошибочных платежей.

В системе «КиберПлат» (CyberPlat®) за 20 лет функционирования не произошло ни одного случая взлома транзакции.

АППАРАТНАЯ МНОГОПЛАТФОРМЕННОСТЬ

Значительными достижениями системы электронных платежей «КиберПлат» (CyberPlat®) является возможность выбора способа оплаты и использование различных устройств для проведения платежа в зависимости от возможностей агентов.



Оплата может осуществляться через кассира, использующего:

- подключённый к интернету компьютер или смартфон (к примеру, в дилерской компании), осуществляющий платёж через сайт системы «КиберПлат» (CyberPlat®);
- автоматизированный кассовый аппарат (к примеру, в магазине розничной сети) — в этом случае взаимодействие с системой «КиберПлат» (CyberPlat®) осуществляется через сервер торгового предприятия;
- другие аппаратные средства;



При этих операциях поддерживается технология «1С: Предприятие»:

Без участия человека:

- платёжные терминалы;

Через Интернет-Банк-Клиент:

- подключённый к интернету компьютер банка с помощью банковской системы Интернет-Банк-Клиент;
- POS-терминалы;
- смартфоны и телефоны, поддерживающие Java, iOS и Android;
- банкоматы;
- мобильные витрины.



Например:

- для торговых сетей используются кассовые терминалы;
- для сети «Эльдорадо» — специальная технология с использованием внутренней сети компании;
- крупные розничные сети («Связной», «Евросеть», сеть салонов МТС, Tele2 и др.) применяют решение на основе 1С или собственных разработок;
- сети магазинов электроники («Эльдорадо», «Технодом» и др.).

Система «КиберПлат» (CyberPlat®) ведёт детальный учёт всех операций при использовании любого из перечисленных механизмов, а полная статистика платежей доступна в режиме онлайн администратору агента на сайте компании <http://www.cyberplat.ru>.



ПОВЫШЕННЫЕ ОТКАЗОУСТОЙЧИВОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

Эксперты «КиберПлат» (CyberPlat®) постоянно тестируют производительность и устойчивость работы системы. Возможности системы существенно опережают самые жёсткие технические требования рынка приёма платежей по всем параметрам. В результате модернизации технологической платформы системы электронных платежей её производительность превысила рекордные 1400 транзакций в секунду. По показателю отказоустойчивости «КиберПлат» (CyberPlat®) превосходит аналогичный показатель ближайшего конкурента системы более чем в 5 раз. Это совершенно уникальный показатель для российского рынка приёма платежей.



**Скорость:
1400
транзакций
в секунду**

Даже в пиковые моменты загрузки «КиберПлат» (CyberPlat®) (в том числе когда из-за технических сбоев не действуют другие платёжные системы и поток платежей через «КиберПлат» (CyberPlat®) значительно возрастает) максимальная нагрузка на систему не превышает 110 транзакций в секунду. То есть возможности системы обеспечивают более чем 14-кратный запас по отношению к рабочим пиковым уровням нагрузки на систему. «КиберПлат» (CyberPlat®) впервые в отраслевой практике предоставила доступ к сервису нагрузочного тестирования действующим и потенциальным партнёрам. Нагрузочное тестирование выполняется в промышленной системе с использованием её дополнительных мощностей, свободных от проведения текущих платежей.

В отличие от потока реальных операций взаимодействие с внешним провайдером имитируется программно внутри системы. Каждый тест отображается интерактивным графиком и текущими результатами измерения производительности. Продолжительность одного нагрузочного тестирования составляет от 1 минуты 40 секунд до 13 минут 40 секунд при обработке от 100 тысяч до 1 миллиона транзакций. Стоимость сервиса за одну транзакцию составляет 1 копейку. Оплата услуги производится банковскими картами VISA и MasterCard, через «Платёжную книжку» «КиберПлат» (CyberPlat®) или через приложения электронной коммерции ведущих российских операторов сотовой связи.

КРУГЛОСУТОЧНАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

В целях обеспечения бесперебойности бизнес-процессов в сети приёма платежей «КиберПлат» (CyberPlat®) в компании создана служба круглосуточной технической поддержки, специалисты которой всегда готовы дать необходимые консультации и оказать экстренную техническую помощь в следующих случаях:

- при сбоях и проблемах в настройке программного обеспечения для платёжных терминалов и для касс торговых предприятий;
- в случаях необходимости уточнения статуса платежей;
- при сбоях в работе операторов связи или неполадках в биллингах тех или иных провайдеров;
- по любым другим проблемам, связанным с нарушением процессов и процедур приёма платежей.

ЗАКОННОСТЬ И НЕОСПОРИМОСТЬ ОПЕРАЦИЙ

Использование электронной цифровой подписи с длиной ключа 1024/2048 бит исключает риски мошенничества и делает операцию по пополнению лицевого счёта в биллинге оператора неоспоримой.

СЕРТИФИЦИРОВАННОСТЬ

Программное обеспечение системы электронных платежей «КиберПлат» (CyberPlat®) сертифицировано уполномоченными государственными органами. Процессы в системе электронных платежей «КиберПлат» (CyberPlat®) сертифицированы компанией «КПМГ Лимитед».



ОТСУТСТВИЕ КОНКУРЕНЦИИ С СОБСТВЕННЫМИ ПАРТНЁРАМИ (ПЛАТЁЖНЫМИ АГЕНТАМИ)



Система электронных платежей «КиберПлат» (CyberPlat®), будучи процессинговой компанией, не имела и не имеет собственных точек приёма платежей — ни в виде терминальной сети, ни в виде сети розничных пунктов приёма платежей, в отличие от других платёжных систем. Исключением является небольшая сеть терминалов приёма платежей, предназначенная для

проверки и тестирования программного обеспечения, а также новых платёжных сервисов и продуктов. Таким образом исключается конкуренция со своими же агентами, имеющая место у других платёжных систем.

Поэтому агенты, работающие через систему электронных платежей «КиберПлат» (CyberPlat®), не сталкиваются со случаями:

- получения конкурентами информации об оборотах по сети и по отдельным точкам приёма платежей, которая может быть использована в конкурентной борьбе;
- попыток недружественного поглощения с использованием полученной информации и методов недобросовестной конкуренции (административный ресурс, рейдерские захваты, коррупционные схемы);
- попыток вытеснения с наиболее прибыльных точек, в том числе с использованием такого метода недобросовестной конкуренции, как демпинг.
- Именно по этой причине многие сети платёжных терминалов, работавшие через другие платёжные системы, перешли на обслуживание в систему электронных платежей «КиберПлат» (CyberPlat®).

ОТСУТСТВИЕ ПРАКТИКИ ПРОДВИЖЕНИЯ СОБСТВЕННОГО БРЕНДА ЗА СЧЁТ БРЕНДОВ ПАРТНЁРОВ

Система электронных платежей «КиберПлат» (CyberPlat®) оказывает услуги прежде всего как процессинговая компания и не имеет собственных точек приёма платежей. Поэтому компания «КиберПлат» (CyberPlat®), работающая в сегменте B2B, не продвигает свой бренд в среде конечных пользователей (плательщиков) в отличие от других платёжных систем. Конкуренты системы электронных платежей «КиберПлат» (CyberPlat®) в большинстве случаев являются самостоятельными игроками на рынке розничных платежей и потому крайне заинтересованы в продвижении собственного бренда в клиентской среде, а также в ослаблении и вытеснении других брендов с рынка. Это вызывает прямой конфликт интересов такой процессинговой компании и её партнёров-агентов.

Нередко одним из основных требований при подключении менее крупного партнёра является его обязательный переход на работу под общим для этой системы брендом, что в перспективе может привести к недружественному поглощению всего бизнеса компании-партнёра.

В случае сотрудничества с системой электронных платежей «КиберПлат» (CyberPlat®) таких проблем не возникает.

ОТСУТСТВИЕ ПРАКТИКИ ПРОДВИЖЕНИЯ И НАВЯЗЫВАНИЯ СВОИМ ПАРТНЁРАМ НЕНУЖНЫХ ИЛИ НЕВЫГОДНЫХ ПРОДУКТОВ И СЕРВИСОВ

Система электронных платежей «КиберПлат» (CyberPlat®) максимально заинтересована в развитии бизнеса своих партнёров, поскольку не имеет собственных точек приёма платежей.

Доходы системы напрямую зависят от оборотов её партнёров, поэтому «КиберПлат» (CyberPlat®) в отличие от конкурентов не продвигает и не навязывает своим партнёрам такие продукты и услуги, которые были бы выгодны системе электронных платежей, но невыгодны её партнёрам. К примеру, на рынке хорошо известна модель, когда партнёры принудительно обязываются поддерживать в своих терминалах персональные сервисы, разработанные платёжной системой.

Эксплуатация этого сервиса в терминальных сетях партнёров не только не приносит им доходов, но и сокращает обороты по основным платежам. Партнёрство с системой электронных платежей «КиберПлат» (CyberPlat®) исключает подобную практику.

МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ ИТ-ПЕРСОНАЛА

Одним из важнейших факторов, гарантирующих высокую надёжность работы системы электронных платежей, является действующая в компании система материального стимулирования ИТ-персонала, связывающая размер начисляемой ежемесячно премии с показателями бессбойности и онлайнности работы процессинга.

Если доля транзакций, проводимых не в режиме онлайн, составляет более 0,1%, то ИТ-персонал на 100% депремируется, если этот показатель менее 0,01%, то премия выплачивается в полном объёме.

В случае если параметр бессбойности-онлайнности находится в диапазоне 0,01–0,1%, работает линейная шкала начисления премии.



УСТОЙЧИВОСТЬ И МАСШТАБИРУЕМОСТЬ ТЕХНИЧЕСКОЙ ПЛАТФОРМЫ

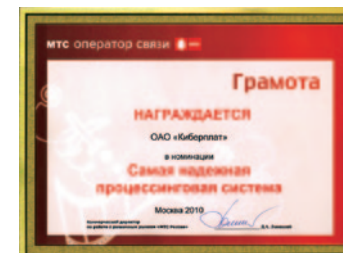


Высокие показатели работы системы обусловлены следующими факторами. Система «КиберПлат» (CyberPlat®) базируется на двух дублирующих друг друга процессинговых центрах, расположенных на территории России. Основной процессинговый центр находится в Москве. Связь между центрами и каналы в интернете дублируются через сети независимых провайдеров связи. Такая система резервирования в сочетании с современной кластерной архитектурой обеспечивает высокую отказоустойчивость «КиберПлат» (CyberPlat®) и независимость от большинства форс-мажорных обстоятельств.

«КиберПлат» (CyberPlat®) предъявляет самые высокие требования к работе программного обеспечения, гарантирующего высокое качество и производительность каждого отдельно взятого модуля и всей системы в целом.

Кроме того, «КиберПлат» (CyberPlat®) успешно работает уже на протяжении более 20 лет, и за этот период система была отлажена и оптимизирована, доработаны и отшлифованы её важнейшие модули.

«КИБЕРПЛАТ» (CYBERPLAT®) РАБОТАЕТ ВСЕГДА!



Надежность системы «КиберПлат» (CyberPlat®) является непревзойденной на рынке России и стран СНГ. Так, ведущий российский оператор сотовой связи МТС в результате комплексного мониторинга своих крупнейших партнёров по приёму платежей признал «КиберПлат» (CyberPlat®) самой надёжной процессинговой системой России и стран СНГ. Данные исследования регулярно проводятся по заказу МТС специалистами независимой экспертной компании по эффективной и проверенной методике.

«КиберПлат» (CyberPlat®) имеет наивысший ресурс отказоустойчивости, надёжности и скорости среди всех платёжных систем. Уже сегодня возможности «КиберПлат» (CyberPlat®) существенно опережают самые жёсткие технические требования рынка приёма платежей по всем параметрам показатель отказоустойчивости системы превосходит аналогичный показатель ближайших конкурентов более чем в 5 раз.

**ОТКАЗОУСТОЙЧИВОСТЬ СИСТЕМЫ «КиберПлат» (CyberPlat®) —
ВНЕ КОНКУРЕНЦИИ!**

ПРОВЕРКА ПОЛУЧАТЕЛЯ

Преимуществом технологии системы электронных платежей «КиберПлат» (CyberPlat®) является проведение платежа в два этапа. Сначала производится обязательная авторизация платежа — в режиме реального времени направляется запрос в биллинговую систему оператора о наличии номера абонента. Только в случае получения положительного ответа операция по пополнению лицевого счёта абонента может быть корректно выполнена. Не все подобные платёжные системы используют в своей работе двухэтапную схему, что приводит к многочисленным ошибкам и претензиям со стороны плательщиков.



ОНЛАЙН (2 СЕКУНДЫ)



Все финансовые операции через систему «КиберПлат» (CyberPlat®) проходят в режиме реального времени, и денежные средства практически мгновенно поступают на счёт получателя платежа. На случай технического сбоя — временной неработоспособности биллинговой системы оператора — в «КиберПлат» (CyberPlat®) функционально предусмотрена возможность накопления платежей до момента начала работы биллинга оператора. Сразу после запуска биллинговой системы все накопленные платежи будут проведены.

ПРОДУКТЫ И РЕШЕНИЯ «КИБЕРПЛАТ» (CYBERPLAT®)

ПРОДУКТЫ И РЕШЕНИЯ ДЛЯ РИТЕЙЛА

ОРГАНИЗАЦИЯ ПРИЁМА ПЛАТЕЖЕЙ (DOMESTIC TOP-UP)

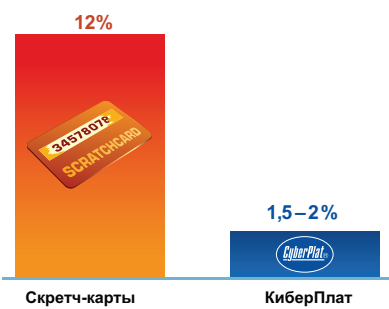
Основой бизнеса системы электронных платежей «КиберПлат» (CyberPlat®) является разработанная и реализованная в глобальных масштабах система организации приёма платежей физических лиц через партнёрскую сеть («нижний сегмент» бизнес-схемы) в пользу широкого круга различных поставщиков услуг и товаров («верхний сегмент» бизнес-схемы). «Нижний сегмент», сеть приёма платежей, составляют предприятия ритейла, банковские офисы и сети банкоматов, сети терминалов самообслуживания.

Количество пунктов приёма платежей в «нижнем сегменте» на конец 2018 года составляло почти 1,5 миллиона. Кроме того, существует достаточно большое число пользователей систем Интернет-Банк-Клиент, принадлежащих банкам — партнёрам системы электронных платежей «КиберПлат» (CyberPlat®), в которые интегрированы возможности по проведению платежей в пользу провайдеров услуг. Такие пользователи также представляют собой часть «нижнего сегмента» системы приёма платежей «КиберПлат» (CyberPlat®).



ОРГАНИЗАЦИЯ ПРИЁМА ПЛАТЕЖЕЙ НА ПРЕДПРИЯТИЯХ РИТЕЙЛА. ПОЧЕМУ ЭТО ВЫГОДНО

НИЗКАЯ СТОИМОСТЬ СБОРА ВЫРУЧКИ



При использовании возможностей системы «КиберПлат» (CyberPlat®) фактическая стоимость сбора выручки значительно снижается, и это крайне важно для операторов. Для скретч-карт стоимость сбора выручки составляет 12% от номинала. Это полная себестоимость, оплаченная оператором за сбор выручки при помощи скретч-карт.

Она включает скидку ритейлерам (обычно 5–6%), затраты на выпуск карт (2–3%), логистику, защиту от мошенничества и целый ряд других

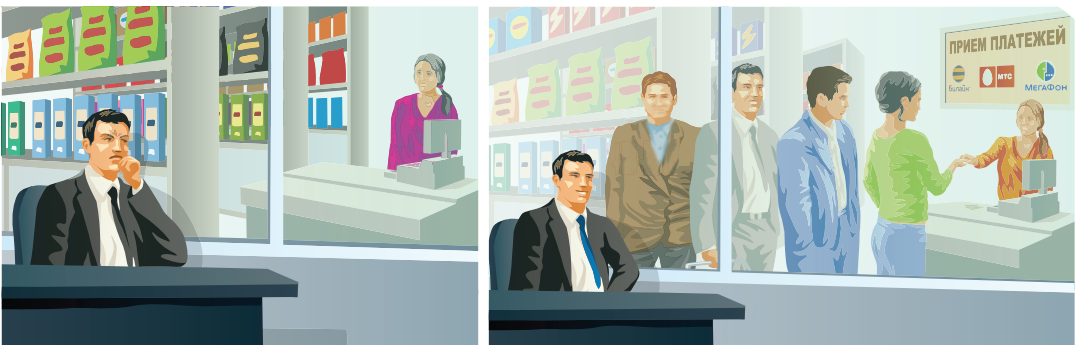
расходов, возникающих при выпуске и распространении скретч-карт.

При сборе платежей через «КиберПлат» (CyberPlat®) в ритейле средняя стоимость сбора выручки за мобильную связь снижается до 1,5–2%. Это огромная экономия для провайдеров услуг.

Экономия 10% дохода такого оператора сотовой связи, как, к примеру, Билайн, чей доход составил в 2018 году \$4,2 млрд, приводит к дополнительной прибыли в \$400 миллионов в год. Это колоссальная сумма.

УВЕЛИЧЕНИЕ ПОТОКА КЛИЕНТОВ И ДОХОДОВ

Многолетний опыт работы системы электронных платежей показывает, что проходимость пунктов обслуживания или торговли, где организован приём платежей через «КиберПлат» (CyberPlat®), увеличивается вдвое. При этом доход от продаж по основному профилю торгового предприятия возрастает на 10–40% в зависимости от качества рекламы и от «профильности» товаров. Например, если в розничной торговой точке продаётся стиральный порошок, то объём продаж стирального порошка увеличится примерно на 10%. Если в торговой точке продаются мобильные телефоны, то увеличение продаж может достигать 40%.



Только ритейл

Ритейл + приём платежей

КАК ПРАВИЛЬНО ОРГАНИЗОВАТЬ ПРИЁМ ПЛАТЕЖЕЙ В РИТЕЙЛЕ

РЕКОМЕНДАЦИИ СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ «КИБЕРПЛАТ» (CYBERPLAT®)

Оборот магазина в значительной степени зависит от того, какое количество людей заходит в него ежедневно. Организация в магазине приёма платежей на кассе в адрес провайдеров различных услуг делает его привлекательным для потенциальных покупателей и увеличивает их лояльность по отношению к торговому предприятию. Все это в итоге приводит к увеличению торговой выручки и прибыли магазина. Клиент, который зашёл в магазин заплатить за мобильный телефон, доступ в интернет, коммерческое телевидение или любые другие услуги, часто делает одновременно и покупки, тем самым увеличивая товарооборот розничной точки.

Многолетний опыт приёма платежей торговыми предприятиями с помощью системы электронных платежей «КиберПлат» (CyberPlat®) показывает, что введение этой услуги увеличивает оборот магазина на 10–40% в зависимости от его профиля, качества рекламы услуги «приём платежей» и степени квалификации обслуживающего персонала. Кроме того, за приём платежей система электронных платежей «КиберПлат» (CyberPlat®) выплачивает магазину комиссионное вознаграждение, которое при правильной организации процесса составляет весьма ощутимую величину.

Для сокращения времени платежа, большего удобства и снижения трудозатрат кассира рекомендуется использовать технологию штрих-кода. Номер телефона абонента трансформируется в штрих-код и для проведения платежа кассиру магазина достаточно пронести карточку через тот же сканер, который считывает штрих-коды товаров.

Соответствующее программное обеспечение имеется в составе пакета, который «КиберПлат» (CyberPlat®) бесплатно предоставляет торговым предприятиям.

Такую карточку «КиберПлат» (CyberPlat®) рекомендует магазину выпустить в рамках своей программы лояльности покупателей, использовать её для собственной рекламы, создания бонусных программ и т.п.

При организации приёма платежей на кассах в розничных точках необходимо учитывать особенности этого процесса. Платёж производится на кассе и требует затрат рабочего времени кассира, хотя и относительно небольших. Если торговая точка находится в посещаемом месте с большой проходимостью покупателей, то в час пик на кассе могут создаваться очереди. Поэтому в такой период «КиберПлат» (CyberPlat®) рекомендует, чтобы кассир принимал платежи на сумму от 500 рублей (за исключением случаев, когда платёж вносит покупатель, который рассчитывается на кассе за покупки в магазине).

Рекомендуется также принимать в это время платежи на меньшие суммы за услуги охранных предприятий или за коммерческое телевидение: платят их состоятельные покупатели, которых магазин должен привлекать дополнительными сервисами, повышая их лояльность по отношению к торговой точке.

В другое время, когда кассиры не перегружены, следует принимать все платежи без ограничений, увеличивая эффективность торгового процесса.

В крупных магазинах с большим количеством покупателей, где кассиры постоянно загружены, целесообразно выделить одну кассу специально для приёма платежей.

Для того чтобы прибыль от приёма платежей была максимальной, необходимо информировать посетителей о возможности заплатить за связь и другие услуги, а также подробно объяснить процедуру проведения платежа.

Услуги по приёму платежей необходимо рекламировать, и чем масштабнее организован этот процесс, тем больший экономический эффект он даст. В начальный период понадобится наружная реклама, чтобы донести до покупателей информацию о появлении на кассах торгового зала новой высокотехнологичной услуги. Позже,





когда посетители привыкнут к этому, она уже не обязательна.

В магазине на кассах рекомендуется размещение наклеек и постеров с логотипами крупнейших операторов мобильной и фиксированной связи, провайдеров других услуг. В супермаркетах следует использовать радиорекламу, периодически воспроизводя аудиоролик с приглашением совершить платёж на кассе торгового зала.

Это способствует текущим и последующим спонтанным решениям посетителей пополнить счёт мобильного телефона или, например, заплатить за услуги коммерческого телевидения или доступ в интернет, услуги ЖКХ и в итоге зайти в магазин, даже если они не собирались этого делать. Если реклама заметна и эффективна, посещаемость магазина после того, как он начинает принимать платежи, может удвоиться.

Для того чтобы организовать приём платежей в магазине, нужно заключить договор с системой «КиберПлат» (CyberPlat®). Этот процесс максимально прост и не требует от владельцев торговых точек больших усилий. Можно подключиться дистанционно через интернет. Для этого надо зайти на сайт <https://customer.cyberplat.ru/dealer/register.html> и зарегистрироваться, а потом прислать по почте необходимые документы. После их подписания выполняется техническое подключение, которое также подробно описано на

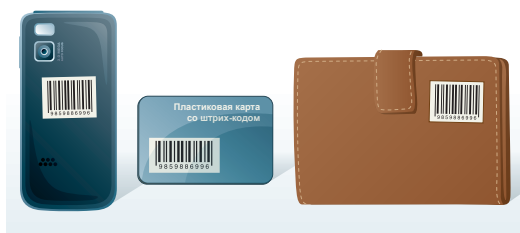
УДОБНАЯ ОПЛАТА

КВАРТПЛАТА КОММУНАЛЬНЫЕ УСЛУГИ

ПОГАШЕНИЕ КРЕДИТОВ

ОСАГО и другие виды страхования

а также: мобильная связь, ТВ, интернет и многие другие платежи



сайте компании. В принципе, при выполнении этих процедур магазин может начать принимать платежи в тот же день, когда произведена регистрация.

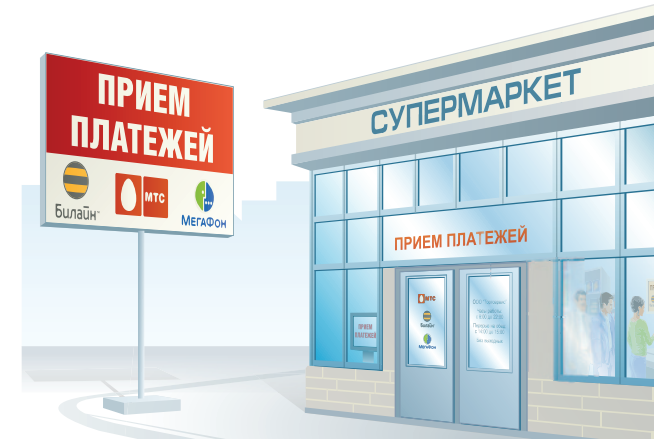
«КиберПлат» (CyberPlat®) предлагает торговым предприятиям широкий ассортимент услуг, в том числе приём платежей за мобильную и фиксированную связь, за услуги операторов доступа в интернет, IP-телефонии и коммерческого телевидения, предприятий жилищно-коммунальной сферы, оплата и бронирование авиабилетов, оплата услуг систем охранной сигнализации и др.

В настоящее время больше всего платежей принимается в пользу операторов мобильной связи, однако другие виды платежей также представляют интерес

для посетителей магазина (и выгодны его владельцу), поэтому их тоже надо предлагать покупателям. Технология «КиберПлат» (CyberPlat®) позволяет принимать платежи, используя широкий выбор оконечного оборудования в соответствии с возможностями владельца магазина.

Кассир для проведения платежа может пользоваться:

- персональным компьютером, подключённым к сети интернет;
- широко распространёнными моделями стандартных кассовых аппаратов;
- программируемым POS-терминалом, который устанавливается на кассе для приёма платежей по банковским картам;
- мобильным телефоном или смартфоном с поддержкой приложений Java, iOS и Android.

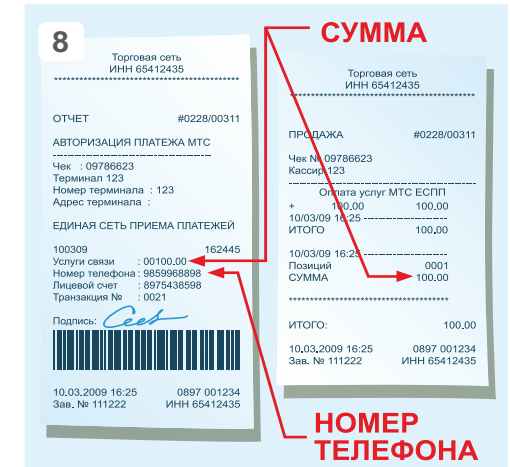
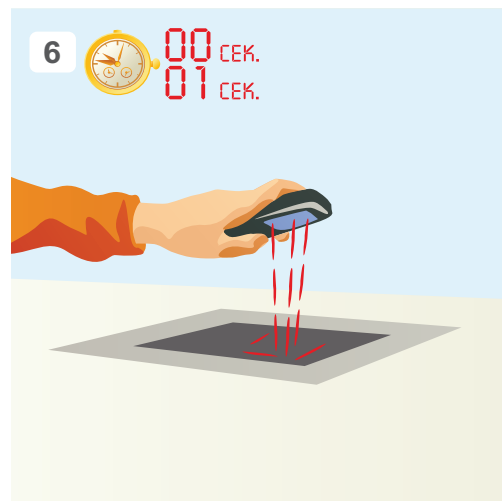
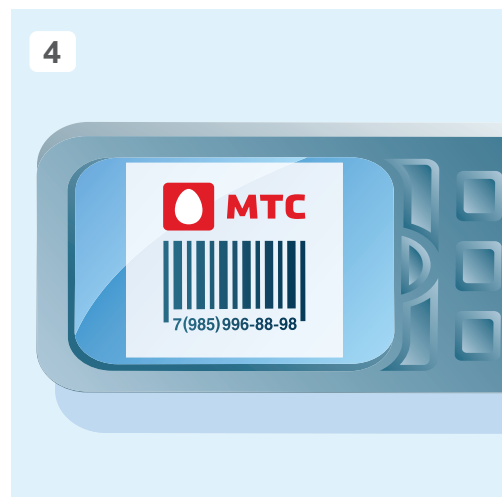
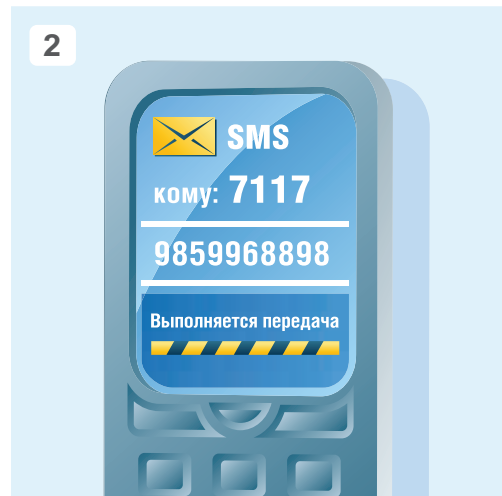


СЕРВИС «СДАЧА НА ТЕЛЕФОН»

Система электронных платежей «КиберПлат» (CyberPlat®) реализовала новый, уникальный для российского рынка электронных платежей продукт — сдача на мобильный телефон при помощи штрих-кода.

При оплате покупки на кассе торговой сети клиент даёт кассиру мобильный телефон, на экране которого находится изображение штрих-кода, либо (что предпочтительней) карту или метку, на которых закодирован номер мобильного телефона, и просит перевести сумму сдачи на его лицевой счёт в расчётной системе оператора связи. Для получения клиентами штрих-кода рекомендуется установить в торговом зале специальный принт-терминал, который описан выше. Распечатав свой штрих-код на метке с липкой основой, клиент сохраняет его, наклеив метку либо на карточку, либо на корпус мобильного телефона, и использует при дальнейших покупках.





Получить личный штрих-код на свой мобильный телефон плательщик может на сайте оператора или на сайте системы электронных платежей «КиберПлат» (CyberPlat®) по адресу <http://card.cyberplat.ru/barcode>, а также на свой мобильный телефон, отправив SMS-запрос на короткий номер 7117 (действует пока только для абонентов МТС, в ближайшее время сервис будет доступен для остальных операторов связи).

Кассир сканирует штрих-код, проводит платёж в режиме онлайн и выдаёт клиенту чек. Для реализации проекта системой электронных платежей «КиберПлат» (CyberPlat®) разработано специальное технологическое решение, которое интегрируется с программным обеспечением для касс торговой сети.

Использование штрих-кода значительно упрощает и ускоряет процесс осуществления платёжных операций.

Эта технология сокращает время обслуживания покупателей, что является весьма критичным для ритейловых сетей с большой проходимостью.

Значительная экономия времени проведения операций делает её привлекательной как для посетителей, так и для торговых сетей.

**ПРИГЛАШАЕМ ТОРГОВЫЕ СЕТИ ПРИНИМАТЬ
ПЛАТЕЖИ И ЗАРАБАТЫВАТЬ ВМЕСТЕ
С СИСТЕМОЙ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ
«КиберПлат» (CyberPlat®)!**

ПРИЁМ ПЛАТЕЖЕЙ С ПОМОЩЬЮ ШТРИХ-КОДА

Стратегическим приоритетом для системы электронных платежей «КиберПлат» (CyberPlat®) является развитие инфраструктуры онлайн-платежей с помощью технологии штрих-кода. Возможность оплаты в торговых предприятиях с помощью штрих-кода не только традиционных товаров, но и таких услуг, как сотовая и фиксированная связь, кабельное телевидение, интернет, жилищно-коммунальные услуги, включая оплату потребляемой электроэнергии, услуги охранных систем и других сервисов, формирует совершенно новый сегмент рынка онлайн-платежей. Широкое внедрение технологий онлайн-платежей, с одной стороны, создаст дополнительные удобства для клиентов, с другой — значительно увеличит доходы торговых предприятий.

Потенциал использования штрих-кодов значительно увеличивается за счёт применения новых технологических решений. Компания «КиберПлат» (CyberPlat®) совместно с компанией IT SERVICE Retail&Banking разработала программно-аппаратный комплекс, позволяющий клиенту самостоятельно распечатывать штрих-коды для платежей по самому широкому спектру услуг — от сотовой связи до погашения кредитов. Установка таких настенных прин-

терминалов в торговых залах позволит значительно ускорить приём платежей на кассах и приведёт к резкому росту платежей за различные услуги в ритейловых сетях.

Значительную выгоду получают те предприятия ритейла, которые первыми организуют приём платежей с помощью штрих-кода на кассах своих торговых предприятий и на торговых площадях.

Система электронных платежей «КиберПлат» (CyberPlat®) предлагает различные способы организации приёма такого рода платежей. Это можно делать непосредственно на кассах, предварительно распечатывая штрих-коды на настенных принт-терминалах, размещённых здесь же, в торговом зале.

Другой вариант — организация отдельных точек по приёму платежей, также оснащённых принт-терминалами. На таких специализированных кассах можно дополнительно организовать приём банковских платежей (погашение кредитов, пополнение депозитных и карточных счетов — причём любых банков), платежей в пользу страховых компаний, отправку денежных переводов. Такого рода точки приёма платежей способны серьезно увеличить доходность торговых предприятий, а также увеличить поток клиентов и за счёт сопутствующих покупок обеспечить рост оборота по основным товарам. Система электронных платежей «КиберПлат» (CyberPlat®) активно продвигает технологии онлайн-платежей в ритейловые сети.

Так, в розничной сети МТС был реализован сервис «КиберСдача», позволяющий с помощью штрих-кода зачислять сдачу от покупок на лицевой счёт абонента, что значительно ускоряет процедуру оплаты на кассе и приводит к росту доходов торговой точки за счёт дополнительно получаемой комиссии.

ПРОГРАММНОЕ РЕШЕНИЕ «МОДУЛЬ ПЛАТЕЖЕЙ» ДЛЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Программное обеспечение «Модуль платежей» устанавливается на компьютеры под управлением ОС Windows для организации приёма платежей на предприятиях ритейла.

В процессе работы программа взаимодействует с интернет-службами «КиберПлат» (CyberPlat®), обеспечивая проведение платежей, а также продажу PIN-кодов через сервис «КиберПлат» (CyberPlat®).

«Модуль платежей» (МП) предоставляет возможность непосредственной печати чеков из программы, поддерживает все популярные типы контрольно-кассовых машин (ККМ).

Программа ведёт реестр принятых платежей и предоставляет большой выбор дополнительных функций, облегчающих приём и последующую обработку платежей.

С более подробным описанием ПО «Модуль платежей» можно познакомиться на сайте системы «КиберПлат» (CyberPlat®): <http://www.cyberplat.ru/tech/online>



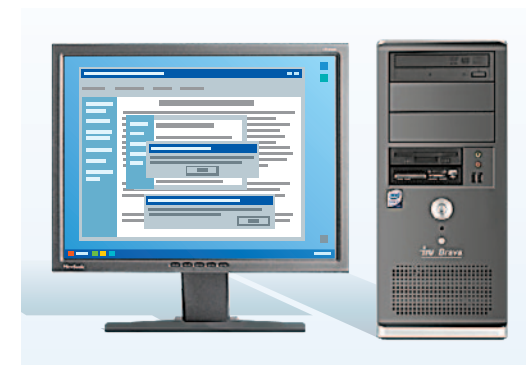
РЕШЕНИЕ ДЛЯ ПОДКЛЮЧЕНИЯ К ПРИЁМУ ПЛАТЕЖЕЙ КАСС ТОРГОВЫХ ПРЕДПРИЯТИЙ

Сервер авторизации платежей (PS) предоставляется системой платежей «КиберПлат» (CyberPlat®) для обеспечения взаимодействия одной или нескольких ККМ или терминалов самообслуживания с центральным сервером системы электронных платежей для организации приёма платежей в торговых предприятиях. PS разработан для платформ Windows и Linux, устанавливается на сервере агента и обеспечивает проведение платежей в режиме реального времени.

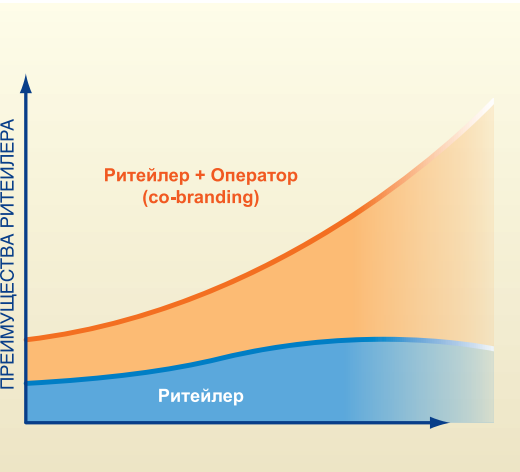
Взаимодействие с центральным сервером системы электронных платежей «КиберПлат» (CyberPlat®) осуществляется по общедоступным каналам интернета.

Защита информации обеспечивается путём шифрования данных и использования электронных подписей. Взаимодействие сервера авторизации платежей с ККМ осуществляется с помощью обмена файлами.

Данное ПО доступно на сайте системы электронных платежей «КиберПлат» (CyberPlat®): <http://www.cyberplat.ru/tech/cashdesk/>



ПОЛУЧЕНИЕ ПРИБЫЛИ ОТ СОВМЕСТНОГО БРЕНДИНГА (CO-BRANDING)



Если сравнивать технологию «КиберПлат» (CyberPlat®) с использованием карточек предоплаты (скретч-карт), то для ритейлера технология «КиберПлат» (CyberPlat®) сокращает расходы на продажи и предоставляет возможность совместного брендинга с теми операторами, в чью пользу организован приём платежей (а это зачастую бренды мирового масштаба).

Сети, которые начинают приём платежей, могут получить бесплатную рекламу от оператора. Например, когда

известный российский ритейлер начал принимать платежи за мобильную связь в своих магазинах, крупнейший российский оператор сотовой связи бесплатно рекламировал эту розничную сеть. Понятно, что совместная реклама всегда выгодна для ритейлера, потому что узнаваемость бренда мобильного оператора всегда выше, а потому он выступает локомотивом продвижения бренда ритейлера.

«КИБЕРСДАЧА» — УНИКАЛЬНЫЙ ФИНАНСОВЫЙ СЕРВИС

«КиберСдача» — современная финансовая технология, связанная с использованием сдачи, оставшейся после оплаты товаров и услуг в розничных сетях, магазинах и мелких торговых точках (www.киберсдача.рф).

Сумма сдачи может быть в режиме реального времени переведена практически любому поставщику услуг без потери времени кассиром с помощью специальной карты «КиберСдача».

Пластиковая карта «КиберСдача» совпадает по размерам со стандартными банковскими картами. На нее нанесены 19-значный номер карты и штрих-код.



Потребитель может перевести сумму сдачи, остающейся после оплаты товаров или услуг, на:

- счёт мобильного телефона;
- банковскую карту;
- расчётный счёт в банке, привязанный к Интернет-Банк-Клиенту (например, на «Платёжную книжку PLAT.RU»).

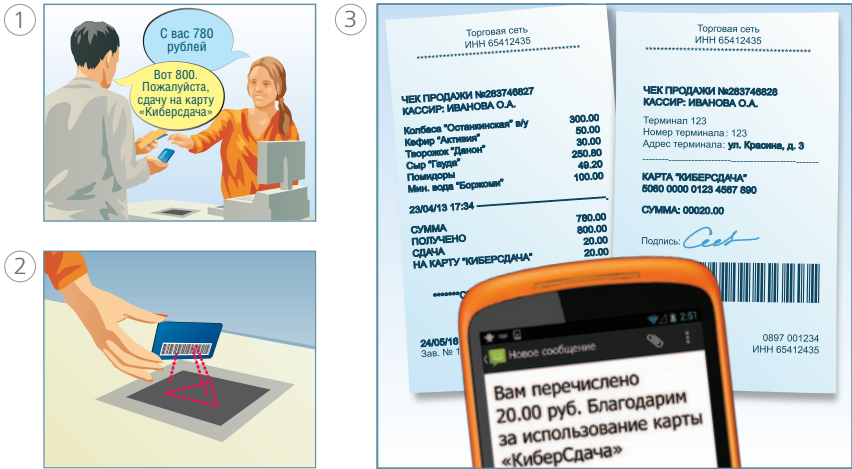
Пользователем сервиса может стать любой человек. Для зачисления сдачи или целевого перевода средств на банковский или лицевой счёт у провайдера услуг необходимо сначала активировать карту «КиберСдача». В процессе активации номеру карты будет присвоен шаблон, содержащий реквизиты платежа, например, код провайдера услуг и номер мобильного телефона либо код банка и номер банковского или лицевого счёта и номер мобильного телефона. Совокупность данных передаётся в систему «КиберПлат» (CyberPlat®) и в дальнейшем служит электронным шаблоном для осуществления переводов автоматически, без ввода реквизитов.

Для операций ниже минимального порога платежа со стороны провайдера клиенту автоматически создается «Платёжная книжка» (www.plat.ru), и сумма сдачи начисляется на неё.

ОБЩАЯ СХЕМА ЗАЧИСЛЕНИЯ СДАЧИ

Рассмотрим часто встречающуюся ситуацию: в самый неожиданный момент мобильный телефон блокируется, потому что заканчиваются деньги. Человек срочно ищет ближайшую точку приёма платежей, чтобы быстро и удобно пополнить счёт.

Он заходит в ближайший магазин известной ритейловой сети и просит кассира пополнить счёт. В ответ кассир предлагает совершить покупку, а сумму сдачи перечислить на счёт сотового оператора. Человек соглашается, так как понимает, что одновременно «убивает двух зайцев»: пополняет счёт, «оживляя» свой телефон, и приобретает нужный товар. В итоге увеличивается оборот магазина и растёт лояльность покупателей к ритейловой сети.



РОСТ ОБОРОТА ВЫСОКОМАРЖИНАЛЬНЫХ ТОВАРОВ

С ростом фут-трафика в результате внедрения проекта «КиберСдача» в торговой точке увеличивается оборот высокомаржинальных товаров. Клиент приходит оплачивать услуги с помощью карты «КиберСдача» и совершает покупки товаров импульсного спроса, обладающих более высокой доходностью, которые расположены в прикассовых зонах.

В электронном ритейле происходит рост продаж аксессуаров: чехлов к мобильным телефонам, брелоков, карт памяти, батареек и т.п.

В продуктовом ритейле растёт реализация пива, сигарет, алкоголя, минеральной воды, шоколада, кондитерских изделий, жевательной резинки, а также увеличиваются продажи непродовольственных высокомаржинальных товаров.

Технология «КиберСдача» подобна японскому сервису «Сдача на карточку». В Японии успешно работает система Felica, в которой сдача от покупок в ритейле зачисляется на карточку бесконтактного считывания. Далее эта карточка может использоваться для оплаты, к примеру, транспортных услуг.

Оборот этой системы в Японии достигает десятков миллиардов долларов — это показывает, что широкое внедрение «Сдачи на телефон» способно значительно увеличить доход операторов. Это будут не миллионы или десятки миллионов, а, скорее всего, сотни миллионов долларов.

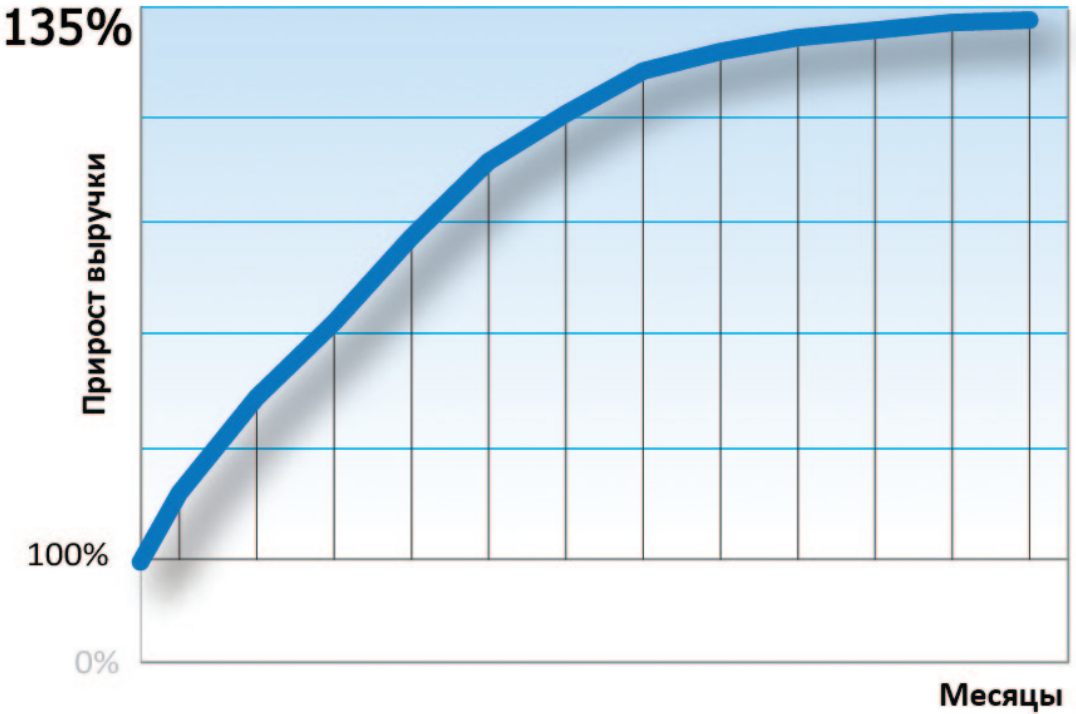
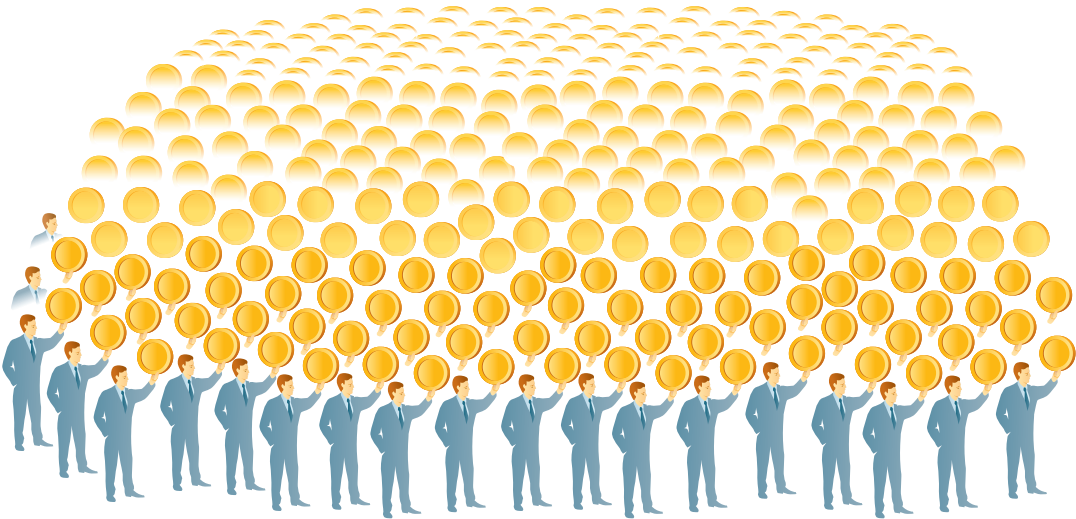


График ожидаемого прироста выручки из-за увеличения фут-трафика



СОКРАЩЕНИЕ ОБОРОТА НАЛИЧНЫХ ДЕНЕГ

Услуга перевода сдачи на счёт мобильного телефона очень выгодна в условиях розничных продаж. Ликвидируются затраты на получение монет из банка, что очень важно, поскольку доставка разменной мелочи и выдача кассирам всегда представляет собой огромную проблему для любого ритейлера.



РЕШЕНИЯ ДЛЯ БАНКОВ

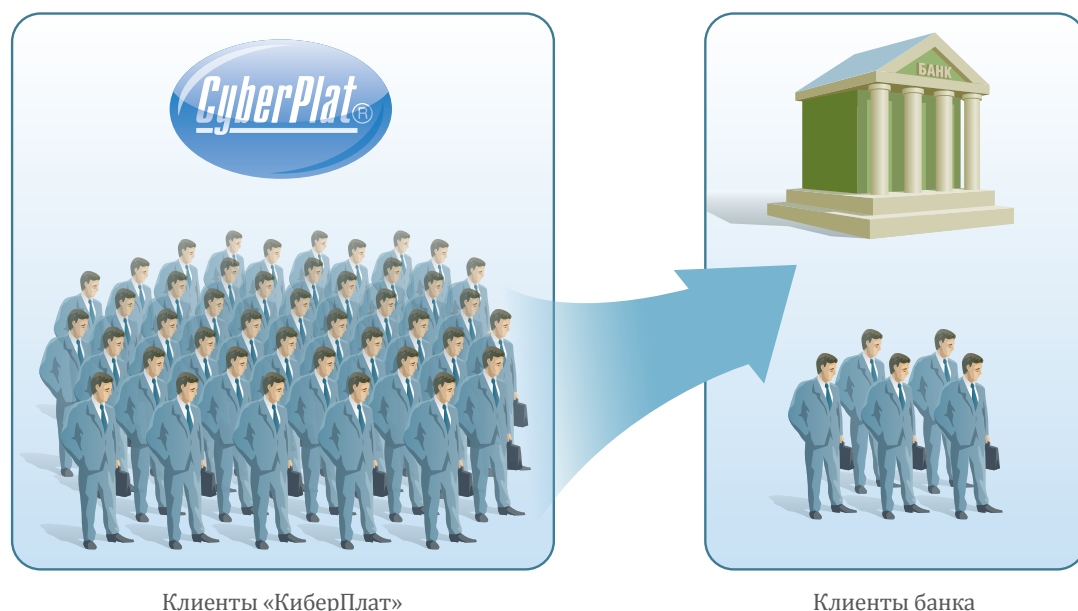
ПРЕДЛОЖЕНИЕ «КИБЕРПЛАТ» (CYBERPLAT®) ДЛЯ БАНКОВ

«КиберПлат» (CyberPlat®) предлагает российским банкам пакет высокотехнологичных сервисов, позволяющих значительно расширить возможности банка по привлечению клиентуры, оптимизации издержек и увеличению прибыли.

«КиберПлат» (CyberPlat®) даёт банкам новую клиентуру. Сотрудничество с системой электронных платежей «КиберПлат» (CyberPlat®) позволит банку получить доступ к новым категориям клиентов — юридическим лицам, являющимся клиентами «КиберПлат» (CyberPlat®), и предложить им свои банковские продукты.

Инкассация торговых и терминальных сетей. Система электронных платежей «КиберПлат» (CyberPlat®) обслуживает очень большое количество предприятий розничной торговли и терминальных сетей, которые принимают наличные платежи на своих торговых точках. В связи с этим клиенты «КиберПлат» (CyberPlat®) имеют потребность в услугах по инкассации и пересчёту денежных средств за принятые платежи в торговых точках. В случае заинтересованности клиенты могут направляться в банк-партнёр.

Краткосрочное кредитование под инкассируемую выручку. Многие предприятия торговли и сервиса, а также владельцы терминальных сетей заинтересованы в получении краткосрочных кредитов для проведения платежей через систему электронных платежей «КиберПлат» (CyberPlat®) в целях покрытия «кассовых разрывов». Такие кредиты в форме овердрафта выгодны банку и практически не создают финансовых рисков, так как обеспечены наличными средствами, которые банк инкассирует в регулярном режиме.



Кредитование терминальных сетей под покупку оборудования (финансовый лизинг). Клиенты системы электронных платежей «КиберПлат» (CyberPlat®) имеют потребности в получении кредитов на закупку оборудования, например cash-in или POS-терминалов. В случае заинтересованности клиенты могут направляться в банк-партнёр.

ПОДКЛЮЧЕНИЕ К СИСТЕМЕ «КиберПлат» (CyberPlat®) — ЭТО НОВЫЕ ВОЗМОЖНОСТИ ЗАРАБОТАТЬ И НОВЫЕ КЛИЕНТЫ ДЛЯ ВАШЕГО БАНКА!

ИНТЕГРАЦИЯ ЭКВАЙРИНГА ПЛАТЁЖНЫХ КАРТ И ПРИЁМА НАЛИЧНЫХ ПЛАТЕЖЕЙ

Банк, осуществляющий эквайринг платёжных карт НСПК «МИР», международных платёжных систем VISA, MasterCard, а также российских платёжных систем, может с помощью системы «КиберПлат» (CyberPlat®) предложить своим клиентам — предприятиям торговли и сервиса — новые возможности. Специальный продукт системы электронных платежей «КиберПлат» (CyberPlat®) интегрирует приём наличных платежей за услуги различных провайдеров и передачу эквайринговых банковских сообщений, связанных с приёмом платежей по банковским картам.

Благодаря этой разработке «КиберПлат» (CyberPlat®) можно совместить в одном устройстве на предприятиях торговли и сервиса приём наличных платежей и транспорт эквайринговых сообщений. При этом используется единый защищённый интернет-канал и единый механизм электронной подписи, который обеспечивает информационную безопасность транзакций.

Использование одного и того же POS-терминала для оплаты покупок по платёжной карте и приёма наличных платежей позволяет избавиться от лишних затрат на оборудование. При этом банк предоставляет продавцу единое средство расчётов с покупателями. Данное решение оптимизирует рабочее место кассира и увеличивает скорость обслуживания покупателей, а покупатели получают дополнительный удобный сервис.



Для реализации единого решения по приёму платежей и процессингу кредитных карт можно использовать POS-терминалы распространённых марок, или персональный компьютер и кардридер.

Основные бизнес-преимущества такого решения для предприятия торговли и сервиса:

- экономия расходов на приобретение аппаратных средств — приём на одном устройстве платежей по картам и наличных платежей;
- гибкость — возможность использования эквайринга любого банка и любого процессингового центра. Переключение между хостами «КиберПлат» (CyberPlat®) и банка производится на уровне терминала;
- дополнительный доход — к обычному эквайрингу добавляется доход от наличных платежей;
- универсальность — реализация как на POS-терминалах, так и на кассовом оборудовании на базе персональных компьютеров.

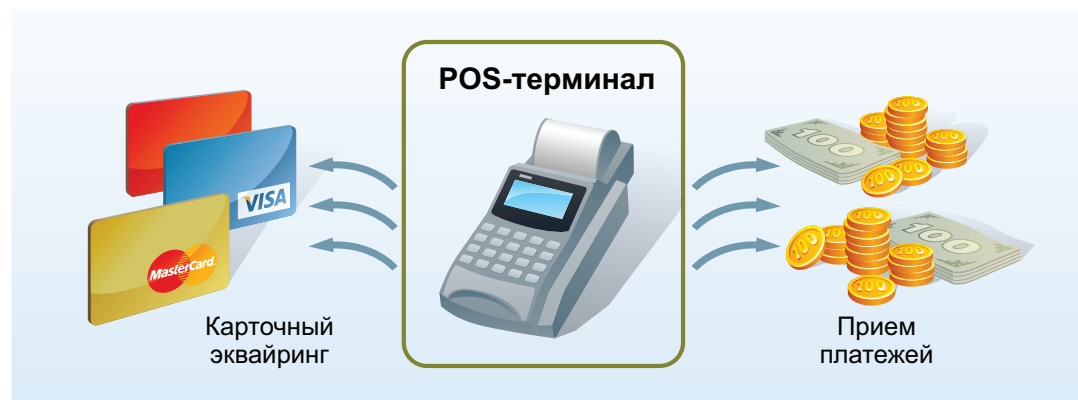
СУЩЕСТВУЕТ НЕСКОЛЬКО ВАРИАНТОВ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ ПРИЁМА НАЛИЧНЫХ ПЛАТЕЖЕЙ И ПЛАТЕЖЕЙ ПО ПЛАСТИКОВЫМ КАРТАМ НА РАБОЧИХ МЕСТАХ КАССИРОВ:

1. Если предприятие торговли и сервиса ведет приём наличных платежей за услуги связи и других операторов с помощью POS-терминала, то достаточно лишь подписать договор с банком на эквайринг платёжных карт. Приобретать новое оборудование за \$400–500 не понадобится.

2. Если для приёма наличных платежей за услуги связи и эквайринг платёжных карт используются два разных POS-терминала, то можно организовать приём обоих видов платежей на одном из них. При этом экономится около \$400–500 (стоимость второго POS-терминала) и также упрощается работа кассира.

3. Если на рабочем месте для приёма наличных платежей используется компьютер, то достаточно подписать договор с банком-эквайером на организацию приёма безналичных платежей и приобрести кардридер за \$90.

4. Если на рабочем месте приём наличных платежей ведётся с использованием компьютера, платежи по пластиковым картам принимаются с помощью POS-терминала и имеется договор с банком-эквайером, то достаточно заменить POS-терминал на кардридер. При этом экономия составит \$300–400, а кассиру не нужно



будет пользоваться двумя разными устройствами (что снизит требования к его обучению и количество ошибок).

Благодаря предлагаемому продукту на банковских POS-терминалах можно принимать широкий спектр платежей, доступных в электронной системе «КиберПлат» (CyberPlat®). Таким образом, увеличивается эффективность работы банковской сети за счёт увеличения доходности, так как к обычному эквайрингу добавляется доход от приёма наличных платежей в адрес более 8 тысяч провайдеров различных услуг.

Предложив такое решение предприятиям торговли и сервиса, банк получит новых клиентов на эквайринг и увеличит обороты по существующим клиентам.

ПРИЁМ ПЛАТЕЖЕЙ



Подключившись к системе электронных платежей «КиберПлат» (CyberPlat®), банк получает возможность организовать для своих клиентов — физических лиц приём платежей в адрес поставщиков различных услуг. Среди них ведущие операторы мобильной и фиксированной связи, провайдеры коммерческого телевидения и интернета, жилищно-коммунальные службы, авиакомпании, системы охранной сигнализации и многие другие.

Для приёма платежей могут использоваться различные каналы с учётом специфики сети сбыта каждого банка.

- Банкоматы

Организация приёма платежей в пользу различных поставщиков услуг увеличивает доходность банкомата в среднем на 25% при меньшей себестоимости операции (не возникает дополнительных издержек, связанных с использованием кэш-диспенсера и необходимостью загрузки денежных купюр для этих типов операций).

Банкоматы и платёжные терминалы ведущих банков используют возможности «КиберПлат» (CyberPlat®).

Чётко обозначившейся тенденцией последнего времени является перенос стандартных операций, в том числе и приёма платежей, в сети банкоматов и принадлежащих банкам платёжных терминалов. Это позволяет разгрузить операционные помещения банков и снизить операционные расходы. Банки фактически расширяют сеть своих розничных точек с минимальными затратами, при этом обслуживание приближается к клиенту как в пространстве, так и во времени: банкоматы и терминалы самообслуживания функционируют круглосуточно.

Крупнейшие банки страны используют возможности по приёму платежей, предоставляемые «КиберПлат» (CyberPlat®). Это банкоматы таких кредитных учреждений,



как Россельхозбанк, банки группы ВТБ, «Альфа-банк», «Росбанк», «Юникредит», АБ «Россия» и многих других. Это сети терминалов Банка «Русский Стандарт», «Бинбанка», «Московского Кредитного Банка» и многих других.

- POS-терминал

Для приёма платежей через POS-терминалы (производства Verifon, PAX, SAGEM, «Штрих-М») система электронных платежей «КиберПлат» (CyberPlat®) предоставляет программное обеспечение, расширяющее функциональные возможности терминала. Программное обеспечение, разработанное «КиберПлат» (CyberPlat®), позволяет кассиру предприятия торговли и сервиса удобно и просто проводить платежи, принимая наличные денежные средства или используя платёжную карту.

- «Банк-клиент»

Приём платежей через систему «банк-клиент», имеющуюся в банке, может осуществляться как через интернет, так и с использованием мобильного телефона (мобильный банк-клиент).

- Мобильный банк-клиент

Для приёма платежей с помощью мобильного телефона система электронных платежей «КиберПлат» (CyberPlat®) предоставляет банку программное обеспечение для мобильных телефонов с поддержкой соответствующего приложения Java, iOS или Android.

АВТОПЛАТЕЖИ — ГОТОВое РЕШЕНИЕ ДЛЯ БАНКОВ

Автоплатёж — это сервис автоматического пополнения счёта мобильного телефона или автоматической оплаты услуг коммунальных и энергосбытовых компаний, а также штрафов ГИБДД с клиентского счёта в банке.

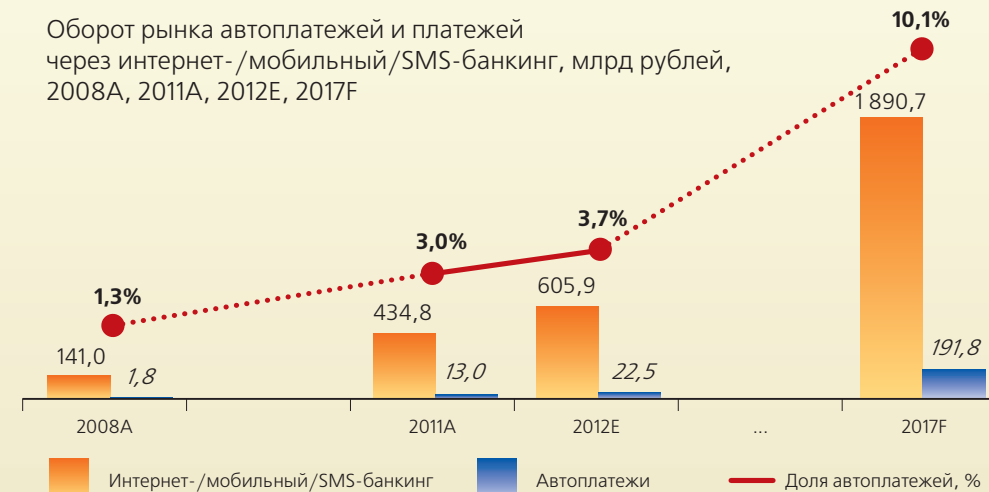
Платёж за сотовую связь осуществляется при снижении баланса счёта до установленного абонентом минимального значения, иные платежи совершаются в соответствии с датами и суммами платежей, установленными самим клиентом.

«КиберПлат» (CyberPlat®) предоставляет услугу в составе комплекса дистанционных финансовых сервисов, включающих:

- интернет-банкинг;
- мобильный банкинг;
- SMS-банкинг.

По оценкам исследовательской компании J'son & Partners Consulting, автоплатежи в России составляют около 10% от оборота платежей всех дистанционных финансовых сервисов.

Оборот рынка автоплатежей и платежей через интернет-/мобильный/SMS-банкинг, млрд рублей, 2008A, 2011A, 2012E, 2017F

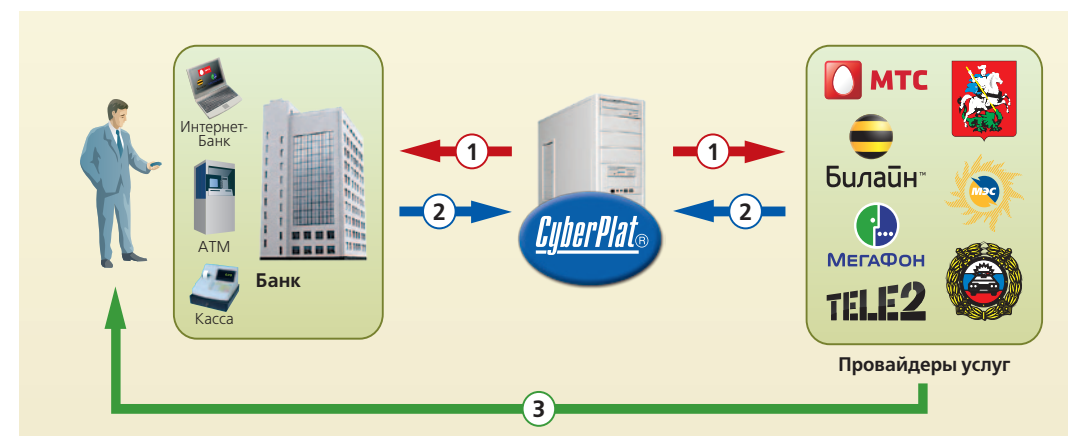


КАК РАБОТАЕТ УСЛУГА

I. Регистрация

1. Клиент отправляет в банк заявку на подключение «Автоплатежа» за услуги требуемого провайдера. Банк через «КиберПлат» (CyberPlat®) направляет заявку провайдеру. Подключить услугу клиент может через систему Интернет-Банк-Клиент, непосредственно в офисе банка, а также в сети банкоматов и терминалов банка.
2. Провайдер через «КиберПлат» (CyberPlat®) подтверждает принятие заявки.
3. Провайдер отправляет абоненту SMS с информацией о подключении услуги.

Дальнейшие настройки характеристик автоплатежа — остаток на счёту, размер суммы пополнения, номер телефона, дата платежа — можно в любой момент скорректировать в офисе банка, в банкоматах и терминалах банка, через Интернет-Банк-Клиент, а также с помощью онлайн-сервиса Plat.ru — Платёжная книжка «КиберПлат» на сайте www.plat.ru.



II. Автоплатеж

Как только возникает необходимость осуществить платёж, банк через систему «КиберПлат» (CyberPlat®) получает запрос от провайдера услуги о проведении платежа.

Со счёта банковской карты клиента производится автоматическое списание средств в размере установленной суммы платежа и зачисление их на счёт получателя платежа.

Клиент банка получает SMS-подтверждение о проведённом платеже.



ПРЕИМУЩЕСТВА ДЛЯ БАНКОВ

- Повышенная ставка комиссионного вознаграждения.
- Рекламная поддержка услуги со стороны компаний МТС, Билайн, МегаФон, Tele2.
- Повышается эффективность использования счетов благодаря увеличению объема клиентских платежей в «своем» банке.
- Растёт лояльность клиентов, так как повышается заинтересованность в поддержании большей суммы остатка для пополнения баланса.
- Сокращается объём снятия наличных для проведения платежей вне банка.
- Привлекаются новые клиенты за счёт предоставления дополнительного сервиса.
- Отсутствуют затраты на разработку: «КиберПлат» (CyberPlat®) предоставляет готовое инновационное решение.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

- Нет необходимости тратить время на пополнение счёта.
- Платёжи зачисляются в режиме реального времени.
- С одного счёта может оплачиваться несколько номеров.
- Возможность проведения автоплатежа, находясь за границей.
- Возможность контроля проведённых платежей в любой момент с помощью отчётов по карте.
- Каждое зачисление средств подтверждается SMS-уведомлением.
- Возможность изменения параметров услуги: остатка на счёту размера суммы пополнения, добавление ещё одного номера телефона.
- Вариативность настроек. Например, график автоплатежа: каждый день, каждую неделю и т.д. либо установка лимита ежемесячной оплаты.
- Бонусные программы от банка.

ПРОДУКТЫ И РЕШЕНИЯ ДЛЯ ТЕРМИНАЛЬНЫХ СЕТЕЙ

ОРГАНИЗАЦИЯ ПРИЁМА ПЛАТЕЖЕЙ В ТЕРМИНАЛЬНЫХ СЕТЯХ



Почему терминальным сетям выгодно работать с «КиберПлат» (CyberPlat®)

Сегодня в России и странах СНГ значительную часть рынка приёма платежей занимают сети терминалов. Как правило, такие сети, развиваясь и укрупняясь, предпочитают работать с системой электронных платежей, не имеющей собственной терминальной сети и заведомо не являющейся конкурентом их бизнесу.

Именно по этой причине многие сети платёжных терминалов предпочитают работать с системой электронных платежей «КиберПлат» (CyberPlat®). Используя программное обеспечение «КиберПлат» (CyberPlat®) клиенты имеют возможность выбора поставщиков услуг, в пользу которых они могут принимать платежи.

При этом система электронных платежей «КиберПлат» (CyberPlat®) в отличие от конкурентов не навязывает своим клиентам сервисы и услуги, которые им не нужны.

Одним из основных преимуществ программного обеспечения для терминалов системы электронных платежей «КиберПлат» (CyberPlat®), которое компания улучшала и совершенствовала в 2018 году, является универсальность, простота установки и использования. Технология открытых кодов позволяет при необходимости дорабатывать приложения под собственные требования крупных сетей, а также дорабатывать приложения «КиберПлат» (CyberPlat®) для их интеграции в учётные системы, системы управления предприятием и бухгалтерские системы клиентов. Это придаёт решениям «КиберПлат» (CyberPlat®) дополнительную гибкость и позволяет им полностью интегрироваться в бизнес-процессы партнёров.

ПРОГРАММНЫЙ КОМПЛЕКС «ТЕРМИНАЛ КЛИЕНТ 3.0.X.X»

Программный комплекс, разработанный и предлагаемый к использованию партнёрами системы электронных платежей, составляют два основных компонента:

- терминальная часть ПО — TerminalClient 3.x.x;
- технический сервис «Мониторинг терминалов».
- TerminalClient 3.x.x устанавливается непосредственно на платёжный терминал.

Технический мониторинг может быть установлен у клиента в офисе или в «КиберПлат» (CyberPlat®).

ПРЕИМУЩЕСТВА ПРЕДОСТАВЛЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- Высокая надёжность, отказоустойчивость, защита от киберугроз.
- Универсальность решения, которая позволяет принимать платежи через большинство типов платёжных терминалов, представленных на рынке.
- Большой и постоянно расширяющийся список поддерживаемого оборудования.
- Поддержка фискальных регистраторов, официально разрешённых к использованию в терминалах.
- Гибкие настройки программного обеспечения.



- Возможность удалённого мониторинга состояния терминалов.
- Несколько вариантов дизайна графического интерфейса.
- Возможность пользователей самостоятельно изменять дизайн графического интерфейса.
- Возможность переключения режимов онлайн и офлайн.
- Приём платежей в пользу операторов, не представленных в системе «КиберПлат» (CyberPlat®).
- Поддержка нескольких типов сторожевых таймеров.
- Открытость исходных кодов программного обеспечения.

Исключительная особенность ПО заключается в возможности приёма платежей в пользу провайдеров услуг, не являющихся операторами системы «КиберПлат» (CyberPlat®), например местных коммунальных служб, интернет-провайдеров и т.п.

ОТКРЫТЫЕ ИСХОДНЫЕ КОДЫ И ТЕХНОЛОГИЯ OPEN SOURCE



Отличительной особенностью программного обеспечения «КиберПлат» (CyberPlat®), которая привлекает крупных клиентов, является наличие открытых кодов разработанных программ.

С 2009 года проект разработки ПО в открытых кодах для платёжных терминалов компании «КиберПлат» (CyberPlat®) перешёл на классическую технологию Open Source. Этот режим разработки программного обеспечения соответствует технологии разработки ПО в таких проектах, как Linux, MySQL и других глобальных программных продуктах.

Отход от концепции разработки программного обеспечения в рамках компании, создавшей продукт, и переход к классическому режиму открытого исходного кода (Open Source) продиктован ростом популярности и масштабов использования разработанного специалистами «КиберПлат» (CyberPlat®) ПО для терминалов. Важным преимуществом предлагаемого продукта является быстрое развитие по сравнению с закрытыми проектами из-за постоянного сотрудничества разных групп разработчиков между собой и сообществом пользователей продуктов Open Source.

Если прежде только специалисты системы электронных платежей «КиберПлат» (CyberPlat®) самостоятельно вносили все необходимые изменения в пакет терминального ПО, то в рамках новой концепции «КиберПлат» (CyberPlat®) предоставляет возможность всем участникам рынка и независимым разработчикам участвовать в совершенствовании ПО. «КиберПлат» (CyberPlat®) при этом выступает модератором и интегратором усилий всех разработчиков, а также владельцем площадки, на которой происходят обсуждение и обмен результатами их деятельности.

С технологической точки зрения проект имеет следующие особенности:

- исходный код версии подготовлен для ОС Windows;
- некоторые компоненты программы представлены в виде бинарных библиотек;
- код предоставляется участникам в режиме «только для чтения», если участник проекта желает сделать свой код доступным, код высылается модераторам для контроля и публикации.

Использование системой электронных платежей «КиберПлат» (CyberPlat®) технологии Open Source при разработке терминального софта обеспечивает лёгкую масштабируемость проекта без увеличения операционных издержек.

Для участия в проекте любой желающий может зарегистрироваться в системе по адресу <https://help.cyberplat.com/>, загрузить проект, получить доступ на запись изменений и записывать изменения по мере их разработки.

ТЕХНИЧЕСКИЙ СЕРВИС «МОНИТОРИНГ ТЕРМИНАЛОВ»

«Мониторинг терминалов» — это комплекс программных средств, разработанный специалистами «КиберПлат» (CyberPlat®), который позволяет получать через веб-интерфейс в режиме реального времени информацию о текущем состоянии терминалов, о состоянии периферийного оборудования, проведённых платежах, ошибках и инкассациях. Кроме того, «Мониторинг терминалов» предоставляет возможность генерировать статистику по этим параметрам.

Применение такой системы позволяет увеличить объём принимаемых платежей и улучшить качество обслуживания клиентов за счёт следующих факторов:

- снижения времени выявления и обработки проблемных платежей;
- своевременного информирования агента о технических неполадках терминалов;
- анализа статистики работы сети.
- Сервис «Мониторинг терминалов» предоставляет следующие возможности:
- в режиме реального времени наблюдать за техническим состоянием сети терминалов, получая информацию по каждому терминалу, в том числе о балансе SIM-карты, исправности принтера и купюроприёмника, наличии GSM-отклика от терминала и т.п.;
- отслеживать сумму платежей, количество внесённых купюр, а также количество платежей и успешность их прохождения;
- перепроводить и отменять проблемные платежи, отслеживать их историю;
- удалённо отправлять на несколько терминалов одновременно команды на выполнение перезагрузки, на получение логов;
- отправлять обновления ПО.





Специалистами «КиберПлат» (CyberPlat®) разработан программный продукт, позволяющий организовать демонстрацию рекламных материалов на основном и втором мониторах терминалов. Это могут быть стационарные или динамические флеш-ролики, продвигающие как собственные услуги и возможности терминальных сетей, так и продукты и услуги сторонних заказчиков.

Решение «Реклама на терминалах» позволяет владельцам терминальных сетей повысить эффективность их бизнеса за счёт:

- привлечения дополнительных клиентов;
- продвижения новых видов услуг (к примеру, приёма коммунальных платежей или платежей в пользу популярных локальных провайдеров);
- получения дополнительного дохода от размещения на мониторах терминалов рекламы сторонних заказчиков;
- укрепления партнёрских отношений с владельцами торговых площадей, на которых расположены терминалы, при рекламе их услуг и продуктов.

ПРИЕМ ПЛАТЕЖЕЙ ЗА ПОГАШЕНИЕ ЗАЙМОВ

Технологические решения «КиберПлат» (CyberPlat®) успешно используют участники рынка услуг микрокредитования в течение нескольких лет. Специально для микрофинансовых организаций (МФО) в рамках ФЗ № 151 «О микрофинансовой деятельности и микрофинансовых организациях», действующего с 2010 года, компания разработала комплекс электронных финансовых сервисов.

ПАРТНЁРЫ

«КиберПлат» (CyberPlat®) работает со многими МФО, включёнными в государственный реестр микрофинансовых организаций, некоторые из них указаны далее.

Благодаря инновационным технологиям «КиберПлат» (CyberPlat®) микрофинансовые организации имеют возможность активно развивать региональную деятельность без привлечения инвестиций на расширение платёжной инфраструктуры.

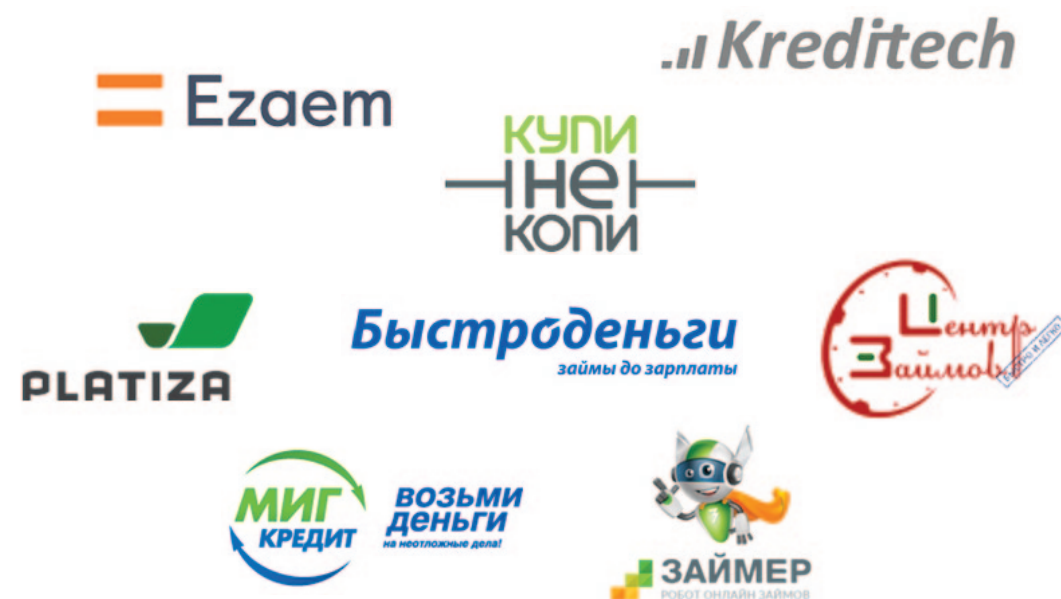


СХЕМА ПРИЁМА ПЛАТЕЖЕЙ В ПОЛЬЗУ МИКРОФИНАНСОВЫХ ОРГАНИЗАЦИЙ

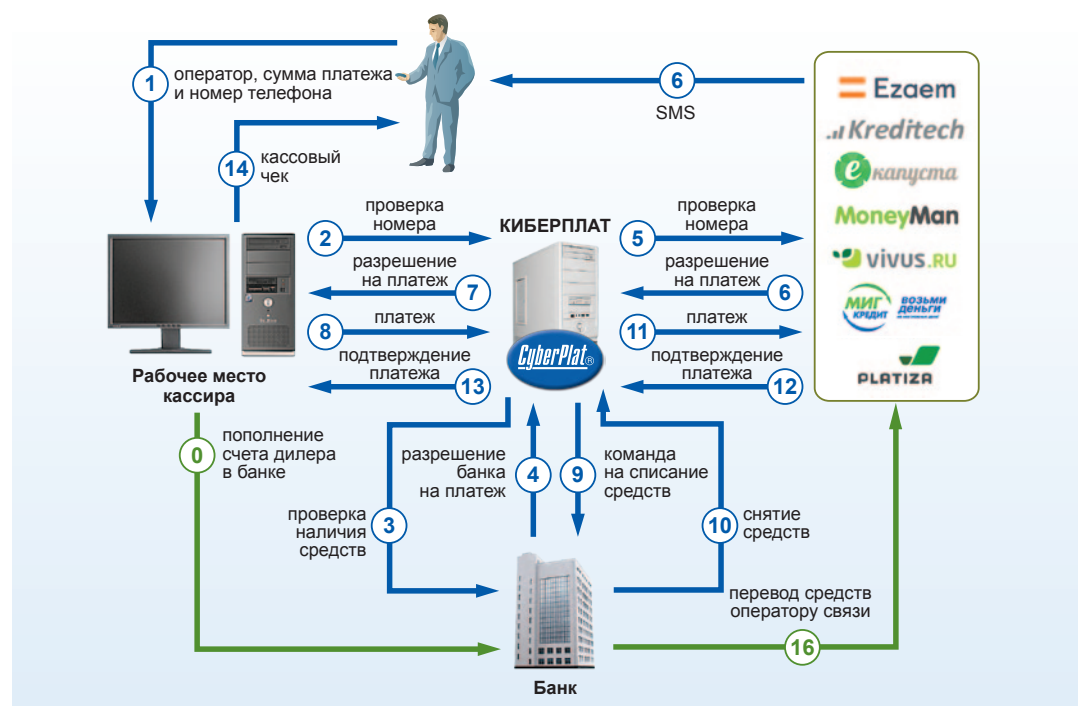
Безопасность транзакций

«КиберПлат» (CyberPlat®) представляет собой систему закрытого типа, в которой все участники расчётов жёстко определены и вывод средств из системы по желанию оператора микрофинансовой организации невозможен.

Каждая операция в системе заверяется электронной подписью, что исключает риски мошенничества и гарантирует безопасность прохождения каждого платежа. Технология CyberCheck использует асимметричный 2048-битный алгоритм кодирования ключей и контролирует каждый этап проведения платежа в режиме онлайн.

ПРИЁМ ПЛАТЕЖЕЙ ЗА ПОГАШЕНИЕ ЗАЙМОВ

«КиберПлат» (CyberPlat®) обладает масштабной платёжной инфраструктурой на всей территории России. Если организация-кредитор не имеет собственной офисной и агентской сети в районе нахождения заёмщиков, МФО может воспользоваться обширной сетью партнёров «КиберПлат» (CyberPlat®) на привлекательных условиях.



ВЫДАЧА ЗАЙМОВ НА БАНКОВСКИЕ КАРТЫ



«КиберПлат» (CyberPlat®) одной из первых на рынке предложила собственное высокотехнологичное решение для выдачи займов на карты международных платёжных систем Visa и MasterCard, а также платёжной системы «МИР». Удобный и безопасный сервис доступен для владельцев карт любого банка-эмитента на территории России.

Преимущества сервиса:

- Бесплатное подключение.
- Минимум временных и организационных затрат.
- Самая низкая комиссия на рынке.
- Партнёрская поддержка 24×7, минимальное время решения проблем.

СЕРВИС УПРОЩЁННОЙ ИДЕНТИФИКАЦИИ ФИЗИЧЕСКИХ ЛИЦ

«КиберПлат» (CyberPlat®) одной из первых в России предоставила микрофинансовым организациям сервис упрощённой идентификации физических лиц с помощью документов, выданных государственными органами.

Для идентификации клиента в системе электронных платежей требуются 2 документа:

1. паспорт гражданина РФ;
2. ИНН либо СНИЛС физического лица.

Полную информацию о потенциальном заёмщике МФО может получить всего за 2 шага, которые потребуют минимум временных затрат и организационных усилий. Для этого микрокредитору необходимо:

1. Заключить договор поручения об упрощённой идентификации с ООО КБ «ПЛАТИНА».
2. Подключиться к системе «КиберПлат» (CyberPlat®).

СЕРВИС РЕЙТИНГОВОЙ ИНФОРМАЦИИ

Сервис рейтинговой информации (составная часть скоринга) предназначен для предоставления данных*, хранящихся в системе электронных платежей «КиберПлат» (CyberPlat®), для анализа качества заемщика в момент выдачи микрокредита. База данных системы содержит более 12 миллиардов записей.

«КиберПлат» (CyberPlat®) предоставляет статистическую информацию о платёжных операциях с идентификацией по телефонным номерам, а также

* Информация не имеет персонального характера по отношению к конкретному физическому лицу.

Информация по номеру телефона		
Номер телефона	926-***-**-84	
Оператор	Мегафон Столица	
Тип отчета	внешний (краткий)	
Период анализа	вся история	
Доминирующий регион	г. Москва	
Критерий	Скоринг	Описание
Существование номера	1	0 - не существует в БД КиберПлат и в биллинге Оператора 1 - существует в БД КиберПлат 2 - нет в БД КиберПлат, но есть в биллинге Оператора
Дата последнего пополнения номера	5	0 - не пополнял давно (больше года) 1 - не пополнял больше 6 месяцев 2 - не пополнял более 3 месяцев 3 - платил в последние 3 месяцев 4 - платил за последний месяц 5 - платил за последние 2 недели
Время жизни номера	4	0 - меньше месяца 1 - больше 3-х месяцев 2 - больше года 3 - больше 3-х лет 4 - больше 5 лет
Сколько всего внесено	6	1 - мало <500 руб 2 - немного 500-1,000 руб 3 - нормально 1,000-5,000 руб 4 - немало 5,000-20,000 руб 5 - много 20,000-50,000 руб 6 - очень много >50,000 руб

ЭКВАЙРИНГ — ОПЛАТА ЗАЙМОВ НА ВЕБ-РЕСУРСАХ МФО

Высокотехнологичное решение «КиберПлат» (CyberPlat®) позволяет в режиме онлайн осуществлять оплату займов с использованием карт международных платёжных систем Visa, MasterCard и НСПК «Мир», эмитированных любым банком на территории России.

- Преимущества сервиса:
- Бесплатное подключение.
 - Самая низкая комиссия на рынке и безупречное качество сервиса.
 - Партнёрская поддержка 24×7, приоритет в решении всех вопросов в кратчайшие сроки.

финансовую информацию о погашении кредитов и пополнении банковских счетов. Информация содержит девять характеристик, объективно определяющих статус потенциального заёмщика.

- Преимущества сервиса:
 - Мгновенная обработка большого объёма данных.
 - Получение ответа на запрос в режиме онлайн.
 - Готовый API-протокол.
 - Бесплатное подключение.
- «КиберПлат» (CyberPlat®) по запросу партнёра бесплатно предоставляет двухмесячный объём данных для проведения тестирования сервиса.

БАНКОВСКИЕ ПРОДУКТЫ

УНИВЕРСАЛЬНЫЕ ШЛЮЗЫ

Изменение законодательства, вступившее в силу с 1 января 2010 года, значительно расширило возможности платёжных систем, сделав доступными те операции, которые прежде могли выполнять только банки. До изменения законодательства можно было принимать платежи по агентской схеме в пользу тех провайдеров, с которыми заключены договоры и организовано информационно-технологическое взаимодействие между учётными системами (разработаны шлюзы). Принятие ФЗ № 121 изменило ситуацию:

«Кредитная организация вправе привлекать организацию, не являющуюся кредитной организацией, и индивидуального предпринимателя (далее — банковский платёжный агент) для принятия от физических лиц денежных средств, направленных органам государственной власти, органам местного самоуправления и бюджетным учреждениям, находящимся в их ведении, в рамках выполнения ими функций, установленных законодательством Российской Федерации, а также на исполнение денежных обязательств физических лиц по оплате товаров (работ, услуг) или для зачисления на их банковский счёт (далее — приём платежей физических лиц), для осуществления операций с использованием платёжных карт, а также для передачи кредитной организации при осуществлении операций с использованием платёжных карт распоряжений физических лиц об осуществлении расчётов по их банковским счетам и составления документов, подтверждающих соответствующие операции, не связанных с осуществлением физическими лицами предпринимательской деятельности и частной практики».

Таким образом, после изменения законодательства стало можно:

- принимать платежи по агентской схеме в пользу тех провайдеров, к учётным системам которых имеются шлюзы;
- принимать платежи по шаблону (банковский провайдер);
- принимать любые платежи за товары, услуги, налоговые, на пополнение банковского счёта физических лиц.

В связи с изменением законодательства специалистами системы электронных платежей «КиберПлат» (CyberPlat®) разработан ряд продуктов и сервисов, позволяющих в максимальном объёме использовать новые возможности.

ПЛАТЁЖИ ПО СВОБОДНЫМ РЕКВИЗИТАМ

На кассах торговых предприятий и в терминалах, подключённых к системе электронных платежей «КиберПлат» (CyberPlat®), можно провести платёж по оплате товаров, работ, услуг, налогов и сборов, а также пополнить банковский счёт, если плательщику известны банковские реквизиты получателя платежа.

Подавляющее большинство крупнейших провайдеров услуг на территории России и стран СНГ уже являются партнёрами «КиберПлат» (CyberPlat®). Эти



операторы зарегистрированы в системе электронных платежей, а «КиберПлат» (CyberPlat®) имеет шлюзы к их учётным системам, что позволяет совершать платежи по упрощённой для клиента процедуре — с минимальным количеством заполняемых на экране платёжного терминала или сообщаемых кассиру торгового зала данных, в большинстве случаев — в режиме онлайн.

Однако на рынке работают и тысячи предприятий, пока не представленных в системе «КиберПлат» (CyberPlat®), предприятия ЖКХ, локальные провайдеры интернета и местного кабельного ТВ, охранные предприятия и платные парковки, детские сады и частные клиники, услугами которых регулярно пользуются миллионы граждан.

Для платежей в пользу такого рода предприятий разработана специальная технология «платежей по свободным реквизитам».

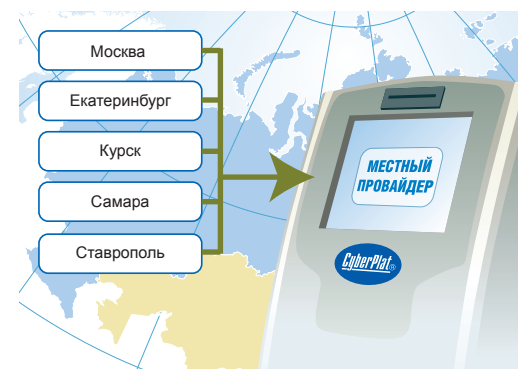
Для совершения «платежа по свободным реквизитам» достаточно знать только банковские реквизиты поставщика или учреждения — получателя денежных средств.

Воспользоваться этим сервисом очень просто — необходимо выбрать тип платежа, заполнить банковские реквизиты получателя и подтвердить проведение операции.

Платёжи «по свободным реквизитам» доступны не только в сети приёма платежей «КиберПлат» (CyberPlat®), но и для пользователей сервиса «Платёжная книжка» (www.plat.ru). В этом сервисе предусмотрена возможность сохранения реквизитов таких платежей, что упрощает дальнейшие операции, сводя их лишь к корректировке суммы, если это требуется.

Платёжи по свободным реквизитам в сети приёма платежей «КиберПлат» (CyberPlat®) — хорошая альтернатива платежам в банковских отделениях. Граждане избавляются от необходимости отстаивать очереди в банках и получают возможность оперативно оплачивать любые разрешенные законом услуги в ритейловых предприятиях, подключённых к системе «КиберПлат» (CyberPlat®).

БАНКОВСКИЙ ПРОВАЙДЕР



В качестве агентов КБ «Платина» (расчётный банк системы «КиберПлат» (CyberPlat®)) партнёрам системы электронных платежей открыта возможность организации приёма платежей в пользу региональных и местных провайдеров жилищно-коммунальных услуг, энергообеспечения, кабельного ТВ, интернета, а также платежей для пополнения банковских счетов. Всем

агентам системы электронных платежей «КиберПлат» (CyberPlat®) открыт шлюз «Банковские провайдеры», через который можно осуществлять такого рода платежи в адрес провайдеров, реквизиты которых заведены в систему «КиберПлат» (CyberPlat®). Кроме того, агенты могут добавлять в систему новых провайдеров из числа наиболее популярных и востребованных в данном городе или регионе — для увеличения оборотов по точкам приёма платежей и роста доходности собственного бизнеса.

Все регистрируемые в системе новые провайдеры становятся одновременно доступны всем агентам «КиберПлат» (CyberPlat®). Каждый агент может выбрать тех поставщиков, платежи в пользу которых наиболее востребованы клиентами.

ПОПОЛНЕНИЕ БАНКОВСКИХ СЧЕТОВ



Широкие возможности для роста оборотов предоставляет и доступный для всех агентов «Мультибанковский кредитный шлюз», через который организуется приём платежей в пользу любого банка на территории Российской Федерации — для пополнения депозитов и карточных счетов, в том числе и с целью погашения кредитов.

Эти возможности реализованы во всем клиентском программном обеспечении «КиберПлат» (CyberPlat®) — в «Модулях платежей» для касс и персональных компьютеров, в программном обеспечении для терминалов самообслуживания.

Для партнёров, использующих собственное программное обеспечение, описание протокола взаимодействия по шлюзам «Банковские провайдеры» и «Мультибанковский кредитный шлюз» можно найти по адресу: https://service.cyberplat.ru/cgi-bin/view_stat.utf/help.cgi

ОТРАСЛЕВЫЕ ПРОДУКТЫ

«КИБЕРПЛАТ» (CYBERPLAT®)

«СТРАХОВАНИЕ» (РЕШЕНИЯ ДЛЯ СТРАХОВОГО РЫНКА)

ПРИЁМ ПЛАТЕЖЕЙ И ПОВЫШЕНИЕ ОПЕРАЦИОННОЙ ЭФФЕКТИВНОСТИ

В настоящее время страховые компании сталкиваются с необходимостью содержания кассовых узлов в офисах продаж, что затрудняет подбор помещений, приводит к затратам на инкассацию, охранные услуги и дополнительный персонал.



Организация приёма денежных средств от контрагентов



Организация приёма денежных средств от страхователей

Организация сбора наличных денежных средств от контрагентов, в первую очередь от страховых агентов, сопряжена со значительными задержками в поступлении денежных средств (до 20 рабочих дней), с рисками доставки агентами наличных денег и характеризуется такими же затратами, как и организация кассового обслуживания в офисах продаж.

Использование продуктов и технологий «КиберПлат» (CyberPlat®) для сбора наличных денежных средств позволяет страховой компании прекратить использование касс в офисах продаж и ускорить поступление денежных средств от контрагентов.

Кроме того, повышается качество клиентского обслуживания. Это становится возможным благодаря переводу платежей по очередным взносам по всем видам страхования, продаваемым в рассрочку, в сеть приёма платежей «КиберПлат» (CyberPlat®).

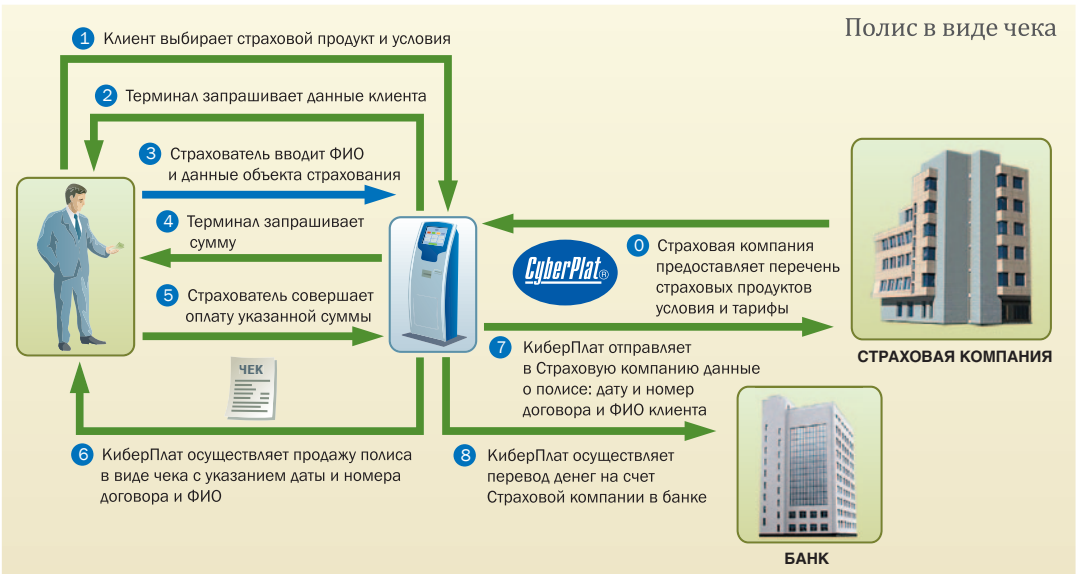
Одновременно снижаются требования к помещениям для организации офисов продаж страховых компаний.

Программно-аппаратные решения «КиберПлат» (CyberPlat®) позволяют внести сумму страховой премии и зачислить сдачу на счёт мобильного телефона страхователя.

В настоящее время проект реализован в страховых компаниях «Росгосстрах», «Ингосстрах», «Хоум Кредит Страхование» и других.

«ПОЛИС В ВИДЕ ЧЕКА» — ПОВЫШЕНИЕ СБОРОВ ПО ВЫСОКОРЕНТАБЕЛЬНЫМ ВИДАМ СТРАХОВАНИЯ

Система электронных платежей «КиберПлат» (CyberPlat®) предлагает организацию продаж безосмотровых страховых продуктов в своих точках приёма платежей. В первую очередь речь идет о «коробочных» продуктах: страховании имущества физических лиц, страховании выезжающих за рубеж и страховании от



несчастного случая. Организация таких продаж возможна на основе заключённого агентского договора между «КиберПлат» (CyberPlat®) и страховой компанией. «КиберПлат» (CyberPlat®) осуществляет продажу «коробочного», безосмотрового страхового продукта в формате чека точки приёма платежей.

При реализации проекта эксперты системы электронных платежей оказывают необходимую методологическую поддержку в процессах разработки и модификации пакета форм страхового документооборота, необходимого для запуска проекта «Полис в виде чека».

В рамках реализации проекта «Полис в виде чека» «КиберПлат» (CyberPlat®) осуществляет агентские платежи за страховые продукты в адрес страховых компаний, удерживая комиссионное вознаграждение в соответствии с агентским договором. При этом обеспечивается передача реестров договоров страхования, содержащих уникальные идентификационные номера оплаченных страховых полисов, включая все необходимые персональные данные (ФИО, адрес, телефон).

«ПАРКОВКИ» (РЕШЕНИЕ ПО АВТОМАТИЗАЦИИ ПАРКОВОК)

Во многих крупных городах России, прежде всего в Москве, существуют серьёзные проблемы с оптимизацией системы дорожного движения, важным компонентом которой стала современная инфраструктура автомобильных парковок. Создание такой инфраструктуры платных парковок сначала в наиболее загруженной центральной части столицы, а затем расширение зоны действия сервиса на все районы города продемонстрировало эффективность этого решения в борьбе с пробками.

Система электронных платежей «КиберПлат» (CyberPlat®) разработала решение с возможностью оплаты парковки из любого магазина, ресторана или кафе, подключённых к «КиберПлат» (CyberPlat®), вне зависимости от того, где припаркован автомобиль.

Решение «КиберПлат» (CyberPlat®) заключается в создании централизованной точки приёма и обработки платежей за парковку и в подключении к этой системе большого количества агентов. В этом случае процедура оплаты за парковку выглядит так.

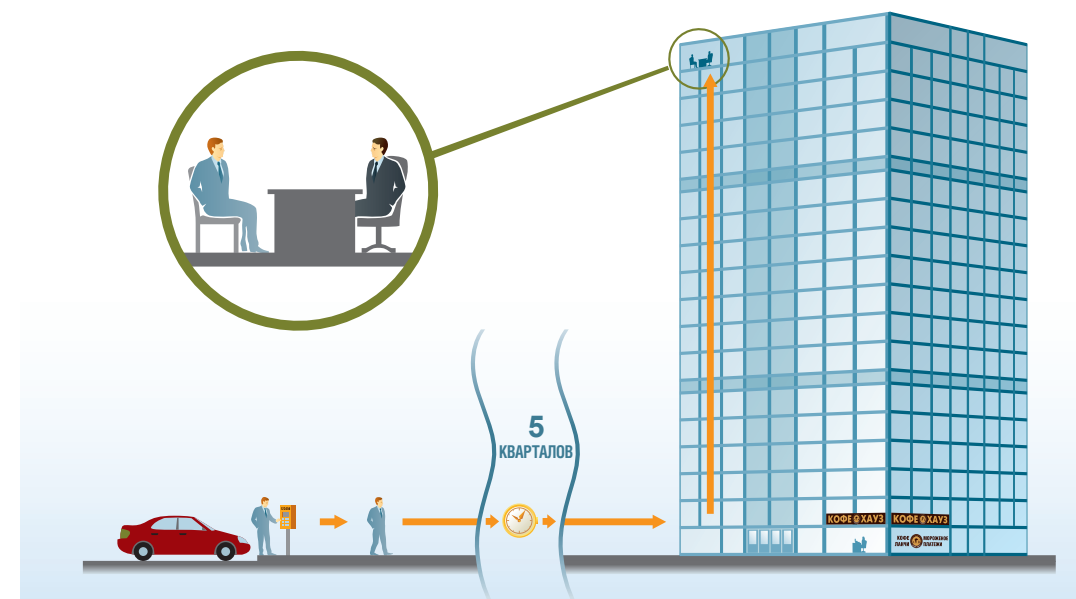


1. Водитель паркует автомобиль на разрешённом месте. Каждое место имеет уникальный номер в рамках региона (например, в рамках города). Номер представляет собой шестизначное число (можно пронумеровать до 999 999 парковочных мест).
2. На парковочных местах, оборудованных парковочными автоматами (паркоматами), водитель может на месте оплатить стоянку по традиционной процедуре.
3. Однако для большего удобства владелец автомобиля заходит в ближайшую точку приёма платежей (это может быть кафе или магазин), называет кассиру номер телефона, ФИО и паспортные данные и вносит деньги. Кассир проводит платёж и выдаёт клиенту чек с данными об оплате. Важно отметить, что оплату (или доплату) можно выполнить из любой точки приёма платежей. К примеру, человек припарковал машину за несколько кварталов от места встречи или работы. Он идёт по своим делам и, если возникла необходимость доплаты за парковку, делает это в ближайшем пункте приёма платежей, не возвращаясь к автомобилю.

Почему это выгодно

Предлагаемое решение очень удобно для клиентов, а также отличается надёжностью, отлаженностью и низкой стоимостью транзакций. Достаточно сравнить альтернативные способы оплаты парковки.

1. Технология оплаты через паркоматы обходится городу приблизительно в 40% от суммы платежей: 20% — эксплуатация оборудования, 20% — стоимость инкассации. Также необходимо учесть затраты на оборудование парковочных мест.
2. Оплата через SMS обходится в 30–40% от суммы платежей — таковы тарифы операторов связи.
3. Оплата карточками (эквайринг) сумм по \$2–3 обходится в 15%.





Стоимость сбора денег по предлагаемой «КиберПлат» (CyberPlat®) технологии первоначально составит 10% с последующим снижением (примерно за два года) ставки до 5%. Уменьшение стоимости будет обеспечено ростом популярности сервиса и, как следствие, снижением стоимости одной транзакции. Данная технология серьёзно заинтересует и предприятия ритейла, кафе, рестораны, магазины, то есть точки шаговой доступности. Привлекательность сервиса для них заключается в увеличении количества клиентов: человек заходит оплатить парковку (ритейлер при этом получает комиссию от платежа), а заодно что-нибудь приобретает либо использует соответствующие услуги.

Общая архитектура системы



Как это работает

Человек припарковал автомобиль на разрешенном для парковки месте. Если место оборудовано паркометром, оплата парковки может быть выполнена на месте.

При необходимости продлить парковку это можно сделать в ближайшей торговой или сервисной точке, подключённой к системе электронных платежей «КиберПлат» (CyberPlat®).

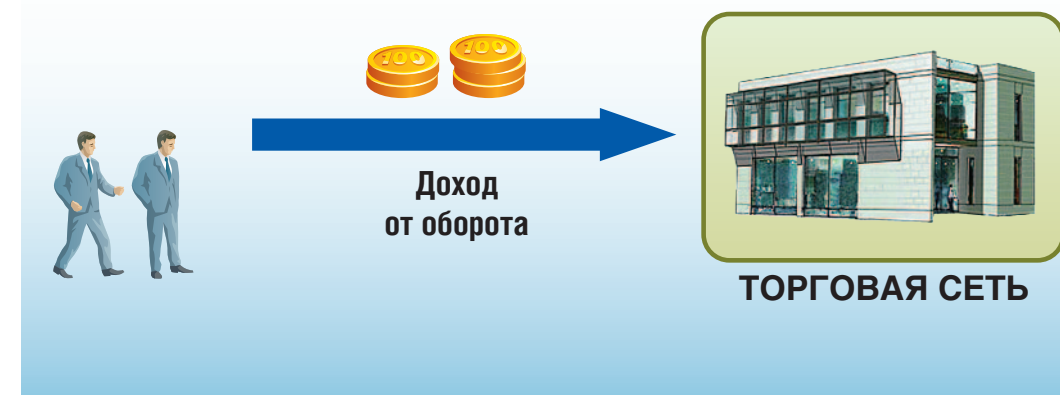
Например, это можно сделать в ближайшей кофейне. Для этого достаточно сообщить кассиру номер парковочного места и продолжительность парковки, а также внести деньги.

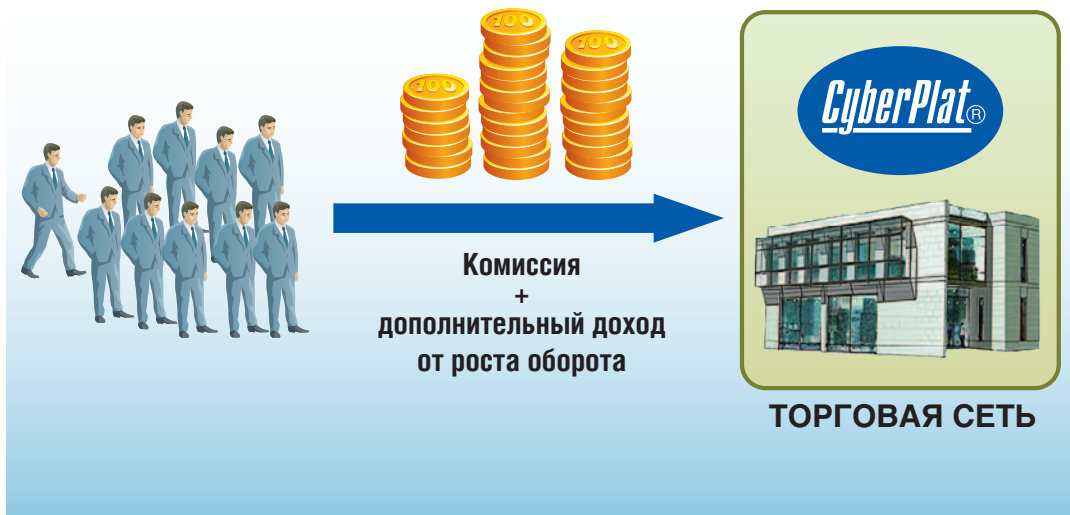
Технология внедрения

Для реализации решения по автоматизации парковок необходимо обеспечить подключение расчётных систем муниципалитетов и крупных частных парковок к процессинговому центру «КиберПлат» (CyberPlat®). При этом необходимости в модификации программного и аппаратного обеспечения муниципалитетов нет. Инфраструктура дилерской сети системы электронных платежей вполне достаточна для немедленного запуска системы — достаточно указать, что только в Москве и в Подмосковье работают 30 тысяч пунктов приёма платежей, подключённых к «КиберПлат» (CyberPlat®).

«ТОРГОВЫЕ СЕТИ» (РЕШЕНИЕ ПО УВЕЛИЧЕНИЮ ПОСЕЩАЕМОСТИ ПРЕДПРИЯТИЙ РИТЕЙЛА)

Специалистами «КиберПлат» (CyberPlat®) разработано решение по стимулированию посещаемости торговых предприятий на основе комплексного использования технологий приёма платежей. Оптимальное сочетание новейших технологий онлайн-платежей позволяет увеличивать посещаемость торговых предприятий и их оборот на 10–40% в зависимости от профиля.

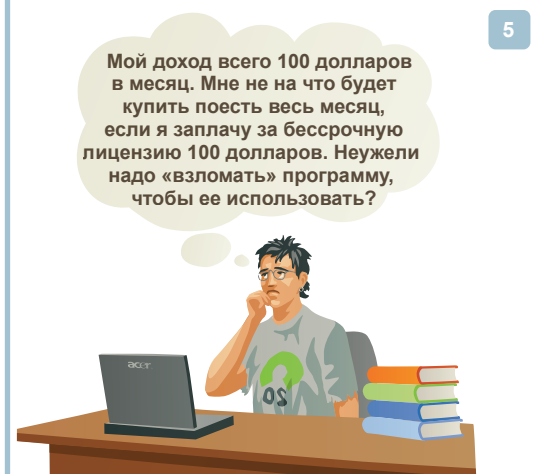
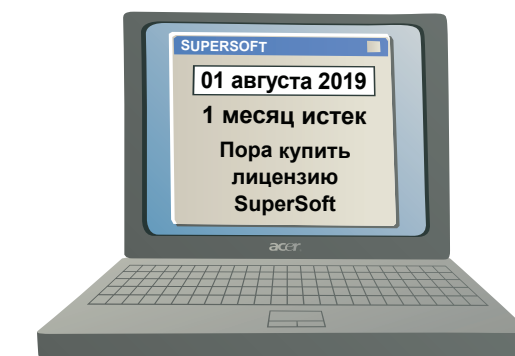
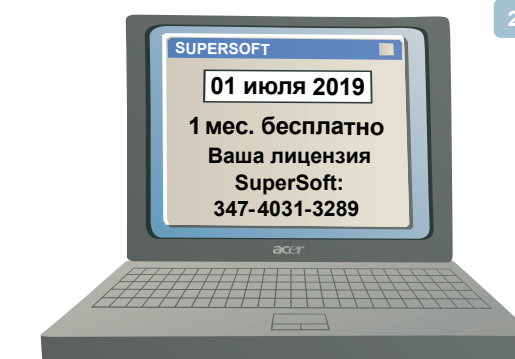


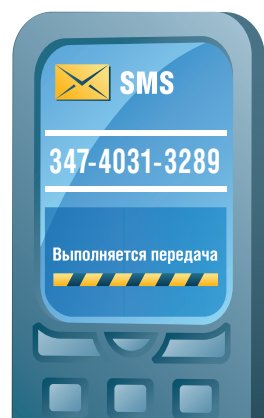
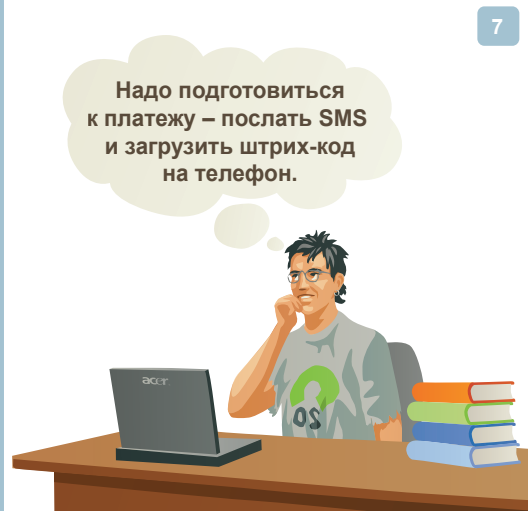


Как показывает опыт «КиберПлат» (CyberPlat®), организация приёма платежей на кассах является одним из основных факторов, увеличивающих клиентский поток. В списке получателей платежей, зарегистрированных в системе «КиберПлат» (CyberPlat®), на конец 2018 года насчитывалось более 8 тысяч провайдеров. Приём платежей воспринимается покупателями как дополнительный сервис, повышающий статус и престижность торгового предприятия. Кроме того, внедрение в рамках решения «Торговые сети» платёжных технологий «КиберПлат» (CyberPlat®) (таких, к примеру, как «КиберСдача») ускоряет обслуживание клиентов, сокращает очереди и делает посещение подобных магазинов более комфортным для покупателей.

Специалистами «КиберПлат» (CyberPlat®) для каждого партнёра из числа торговых сетей разрабатывается индивидуальное предложение в рамках решения «Торговые сети» с учётом специфики каждого предприятия. Для одних сетей для достижения результата — заданных параметров роста посещаемости торговой сети — достаточно внедрения одного-двух сервисов «КиберПлат» (CyberPlat®), для других потребуется использование полного арсенала таких решений и сервисов, для третьих будет рекомендовано дополнительное проведение маркетинговых мероприятий — к примеру, реализация информационных кампаний или специальных программ лояльности для клиентов.

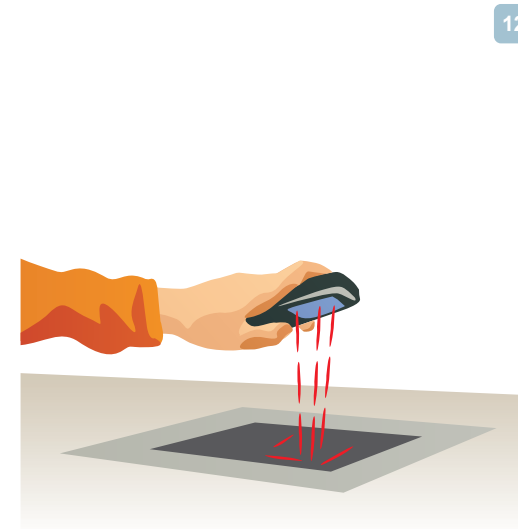
SAAS (ОПЛАТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЗА ВРЕМЯ ПОЛЬЗОВАНИЯ)



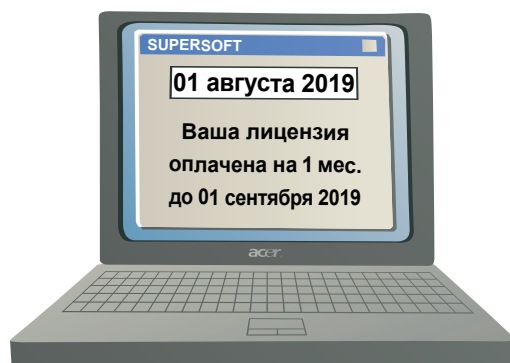


Специалистами системы электронных платежей «КиберПлат» (CyberPlat®) разработана система продажи программного обеспечения, поддерживающая модели как единовременной оплаты лицензии, так и покупки программных продуктов «в розницу», с возможностью работы в режиме SaaS (Software as a Service).

Модель SaaS предусматривает оплату использования программного обеспечения или сервиса только за тот временной период, в который оно необходимо. Таким образом, продукт SaaS представляет собой фактически вариант аренды.



14



Через месяц снова заплачу 2 доллара. 2 доллара в месяц — для меня вполне приемлемо.



15

ИНТЕГРАТОР СИСТЕМ ДЕНЕЖНЫХ ПЕРЕВОДОВ

Интегратор систем денежных переводов (ИСДП) системы электронных платежей «КиберПлат» (CyberPlat®) — универсальный продукт, позволяющий десятикратно увеличить эффективность бизнеса банков в сегменте денежных переводов.

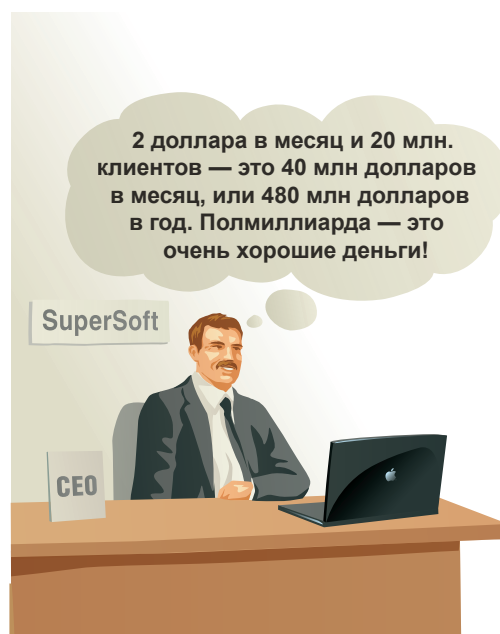
РЫНОК ДЕНЕЖНЫХ ПЕРЕВОДОВ

Анализ развития рынка денежных переводов в разных странах показывает, что со стороны самого широкого спектра потребителей существует растущий спрос на удобный, понятный и доступный сервис денежных переводов с максимальным географическим покрытием.

Глобализация мировой экономики и либерализация рынков труда способствуют дальнейшему росту международного рынка денежных переводов. В любой стране присутствует значительное количество систем денежных переводов. В целях достижения максимальной эффективности работы на чрезвычайно выгодном рынке денежных переводов необходимо охватить по возможности всех потенциальных участников рынка.

КАК МОЖНО ЗАРАБОТАТЬ БОЛЬШЕ

16



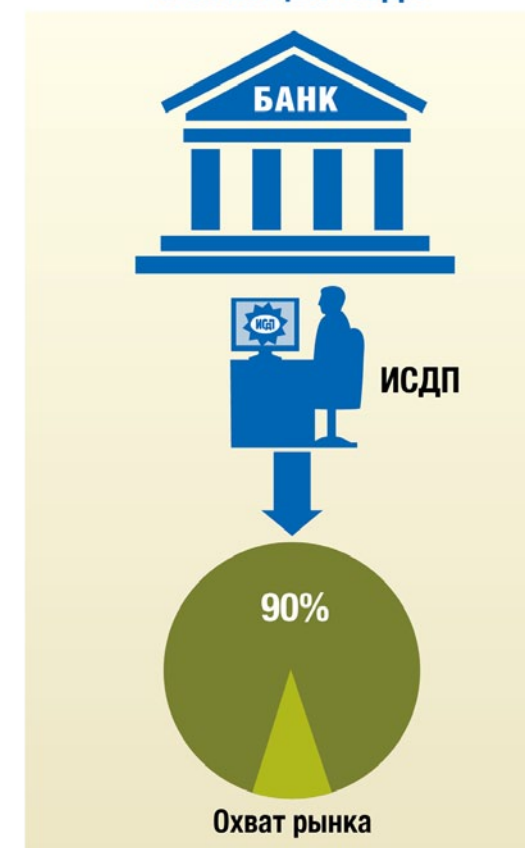
17



Без ИСДП



С помощью ИСДП



Интегратор систем денежных переводов — это универсальный инструмент, позволяющий работать со множеством систем денежных переводов, используя единый интерфейс. ИСДП может быть установлен в банковских офисах, а также на автоматизированных устройствах, например в платёжных терминалах самообслуживания. ИСДП позволяет охватить до 90% потенциальных клиентов без каких-либо серьёзных затрат.

ИСДП успешно эксплуатируется «КиберПлат» (CyberPlat®) с апреля 2008 года. Первый полностью автоматизированный денежный перевод в России был отправлен 8 августа 2008 года с помощью ИСДП, установленного в платёжном терминале Банка «Платина» (расчётный банк системы электронных платежей «КиберПлат» (CyberPlat®)).

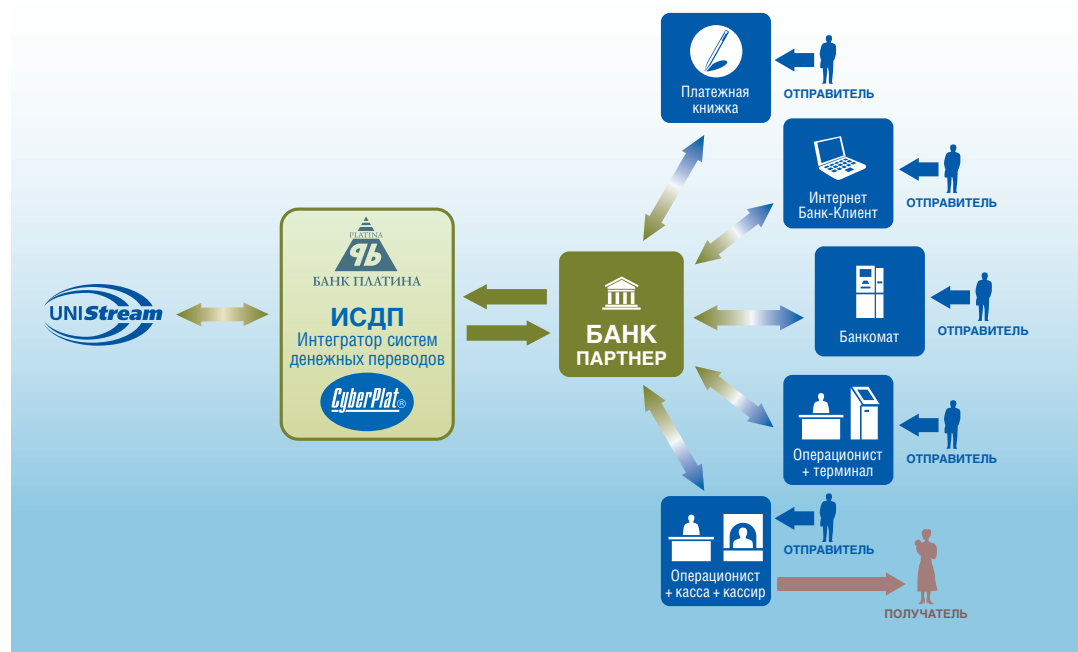
Более 20 банков — партнёров системы электронных платежей «КиберПлат» (CyberPlat®) успешно используют ИСДП для обслуживания клиентов по денежным переводам.

КАК ЭТО РАБОТАЕТ

«КиберПлат» (CyberPlat®) предлагает своим партнёрам единую платформу, интегрирующую не только основные системы русского коридора, но и системы денежных переводов с глобальным присутствием.

Программное решение ИСДП не только может быть установлено на рабочих местах сотрудников в банковских офисах, но и легко инсталлируется на различных устройствах, например в терминалах и банкоматах, позволяющих максимально автоматизировать обслуживание клиентов.

Клиент, пройдя процедуру идентификации в соответствии с требованиями национального законодательства, в дальнейшем получает возможность отправлять



денежные переводы, используя платёжные терминалы, которые работают круглосуточно.

ИДЕНТИФИКАЦИЯ КЛИЕНТА

В соответствии с действующим законодательством клиент, отправляющий денежный перевод, должен быть идентифицирован. Поэтому для отправки переводов через терминалы самообслуживания клиент должен предварительно пройти процедуру регистрации в офисе банка.

1. Клиент предоставляет операционисту банка свой паспорт или иной идентифицирующий его согласно действующему законодательству документ, а также банковскую карту любого банка. Если у клиента нет банковской карты, то он получает её в банке.
2. Операционист вводит в систему «КиберПлат» (CyberPlat®) данные о клиенте, ФИО получателей (до 5), а также названия систем денежных переводов и (при необходимости) адреса точек, куда клиент планирует отправлять переводы.
3. После регистрации клиент может отправлять переводы через терминалы самообслуживания, используя присвоенный ему код (номер карты) и пароль доступа к системе (специальный PIN, не предназначенный для операций по снятию наличных в банкомате).

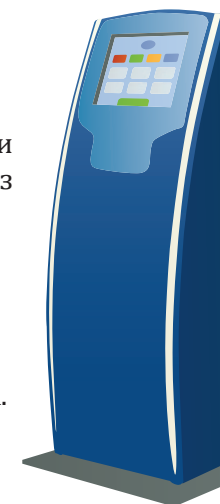
ПОСЛЕДОВАТЕЛЬНОСТЬ ОПЕРАЦИЙ ПРИ ОТПРАВЛЕНИИ ДЕНЕЖНЫХ ПЕРЕВОДОВ

Денежные переводы через терминал

1. Выбрать раздел «Денежные переводы».
2. Ввести на терминале номер карты и выданный при регистрации специальный PIN для доступа к системе через терминалы самообслуживания.
3. Выбрать получателя перевода из списка (до 5 получателей), созданного при регистрации.
4. Внести в купюроприёмник сумму перевода.
5. Подтвердить отправку перевода.
6. Получить и сохранить квитанцию с реквизитами перевода.
7. Сообщить реквизиты перевода его получателю.

Денежные переводы через Интернет-Банк-Клиент

1. Выбрать раздел «Денежные переводы».
2. Выбрать систему денежных переводов.
3. Выбрать получателя перевода из списка или ввести реквизиты нового получателя.
4. Ввести сумму перевода.
5. Подтвердить отправку перевода.
6. Сообщить реквизиты перевода его получателю.



Денежные переводы через банкомат

1. Вставить в банкомат пластиковую карту, ввести PIN-код этой карты.
2. Выбрать раздел «Денежные переводы».
3. Выбрать получателя перевода из списка (до 5 получателей), созданного при регистрации.
4. Ввести сумму перевода.
5. Подтвердить отправку перевода.
6. Получить и сохранить квитанцию с реквизитами перевода.
7. Сообщить реквизиты перевода его получателю.



ОПТИМИЗАЦИЯ РАБОТЫ ОПЕРАЦИОНИСТА БАНКА

Особенностью программного комплекса, предлагаемого системой «КиберПлат» (CyberPlat®) банкам-партнёрам, является удобный интерфейс, который даёт возможность операционистам обслуживать клиентов различных систем денежных переводов в едином окне.

Интегратор систем денежных переводов «КиберПлат» (CyberPlat®) работает в режиме реального времени, поэтому операционисту требуется всего лишь несколько минут для оформления перевода, после чего отправленный перевод становится доступным для получения его адресатом в той системе, которую выбрал отправитель перевода.

Благодаря Интегратору систем денежных переводов банк значительно сокращает время на подготовку персонала. Вместо обучения операционистов использованию интерфейсов каждой из систем денежных переводов достаточно научить их работе с единым интерфейсом для всех систем. При этом снижаются расходы на обучение, нагрузка на операционистов и уменьшается количество ошибок при оформлении перевода.

ЭКОНОМИЧЕСКАЯ ВЫГОДА

Банк получает дополнительную экономию на IT-инфраструктуре: программном обеспечении (один модуль Интегратора систем денежных переводов вместо отдельных модулей для каждой системы денежных переводов), серверах и организации каналов связи. Существенная экономия достигается и за счёт сокращения потребности в квалифицированном персонале финансовых служб банка, так как при работе через Интегратор банк сопровождает только один договор с ООО КБ «ПЛАТИНА» и ООО «КИБЕРПЛАТ» вместо нескольких договоров с разными системами денежных переводов.

Кроме дохода от операций с денежными переводами с использованием ИСДП «КиберПлат» (CyberPlat®), банк может получить значительную экономию от использования терминалов самообслуживания вместо касс в отделениях и филиалах банка. Если приём наличных платежей производится через операциониста, это требует специальной кассовой комнаты с оборудованием стоимостью около \$20 тысяч, плюс дополнительные затраты на аренду помещения и заработную плату кассира.

Сравнение прямых затрат на прием переводов от граждан (по ценам Москвы)

Вид затрат	Прием перевода в банковском офисе	Прием перевода через терминал самообслуживания*
Разовые затраты		
Оборудование точки приема	\$30 000 (операционный зал и касса)	\$13 000 (операционный зал и терминал)
Ежемесячные затраты		
Аренда площадей (минимум)	\$3600 (20 кв.м операционный зал и касса с оборудованными рабочими местами для операциониста и кассира)	\$1800 (10 кв. м операционный зал с оборудованным рабочим местом операциониста. 1 кв.м для размещения терминала в этом случае дополнительно не оплачивается)
Заработная плата	\$3500 (операционист и кассир)	\$1750 (операционист)
Охрана (минимум)	\$3400 (1 сотрудник ЧОП)	Отсутствует (есть дистанционный контроль состояния терминала)
Электроэнергия	\$100	\$50
Итого в месяц:	\$10 600	\$3600

* Ориентировочные затраты для случая, когда терминал самообслуживания находится в банковском офисе без кассового узла и используется вместо кассы.

При использовании вместо кассовой комнаты и кассира терминала самообслуживания затраты составляют \$3000 на приобретение терминала и стоимость аренды 1 кв. м площади. Если же терминал устанавливается в операционном помещении банка, то дополнительные затраты на аренду не возникают.

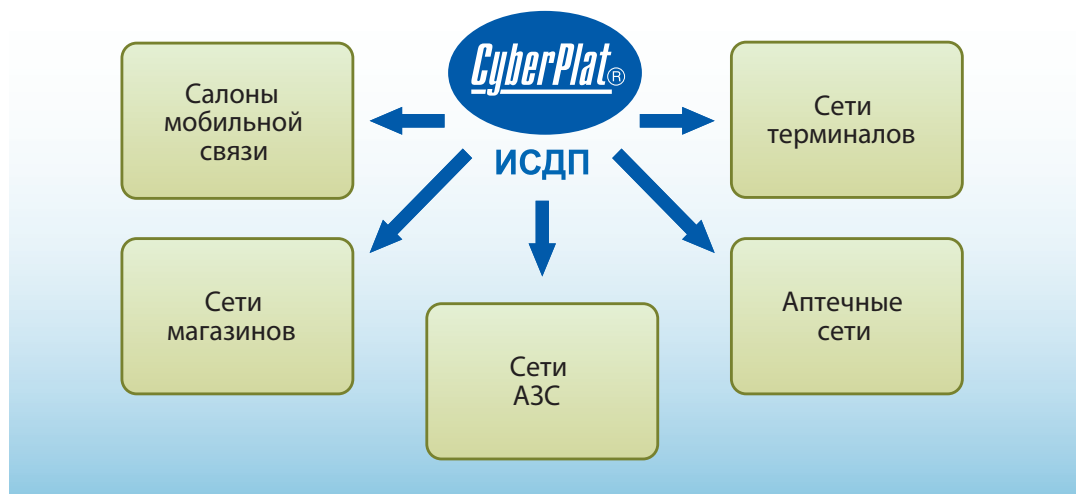
ПЕРЕНОС ФРОНТ-ОФИСОВ ИЗ БАНКА В РОЗНИЧНЫЕ СЕТИ

Если банк начинает принимать денежные переводы через терминалы самообслуживания, он получает возможность перенести этот бизнес из своих операционных помещений в розничные торговые сети. Благодаря этому операционные помещения банка разгружаются от лиц, отправляющих переводы (которые подчас создают неудобства высокодоходным клиентам банка), освобождается время операционистов для проведения более прибыльных для банка операций и обслуживания выгодных клиентов, а также снижаются операционные расходы, приходящиеся на один денежный перевод. Банк фактически расширяет сеть своих розничных точек с минимальными затратами, при этом обслуживание приближается к клиенту как в пространстве, так и во времени: терминалы самообслуживания функционируют круглосуточно.

Использование Интегратора систем денежных переводов системы электронных платежей «КиберПлат» (CyberPlat®) позволит банку:

- внедрить современный, технологичный и недорогой способ обслуживания клиентов с помощью терминалов самообслуживания;
- повысить доступность услуг банка за счёт использования терминалов самообслуживания, расположенных в удобных местах и работающих круглосуточно, 7 дней в неделю;

- увеличить количество переводов и платежей за счёт расширения времени обслуживания клиентов и приближения услуги к потребителю;
- снизить нагрузку на кассиров и операционистов и сократить операционные расходы;
- расширить розничный бизнес и спектр услуг, предоставляемых клиентам банка;
- получить дополнительный доход за счёт операций по банковским картам, выданным банком при регистрации клиента в системе.

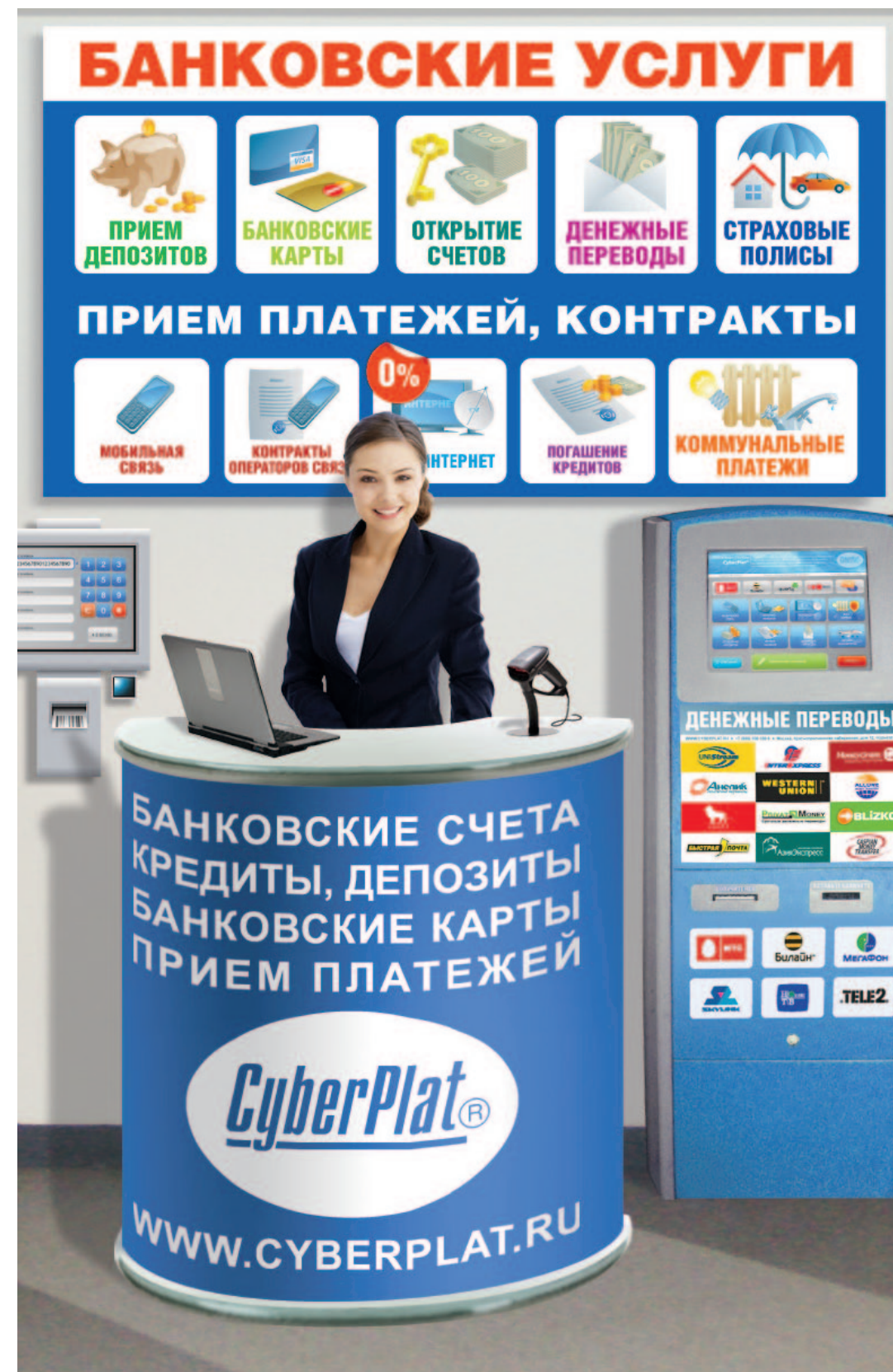


ИСДП В НЕБАНКОВСКИХ СЕТЯХ

Уникальный продукт «КиберПлат» (CyberPlat®) доступен и в небанковских сетях — на кассах торговых предприятий, в салонах связи, аптеках и на автозаправках, а также в платёжных терминалах, подключённых к системе электронных платежей «КиберПлат» (CyberPlat®).

Специальные версии Интегратора систем денежных переводов (ИСДП) для касс, персональных компьютеров и платёжных терминалов предлагаются системой электронных платежей «КиберПлат» (CyberPlat®) своим партнёрам для увеличения оборотов и доходности их бизнеса. Для начала приёма денежных переводов не требуется ни финансовых, ни значительных организационных затрат — достаточно дистанционно обновить действующее программное обеспечение в зависимости от типа используемого оборудования.

Широкое внедрение ИСДП в сети партнёров системы электронных платежей «КиберПлат» (CyberPlat®) делает отправку денежных переводов комфортной и удобной операцией, обеспечивает новый уровень качества обслуживания клиентов в точках шаговой доступности.



КУБ: КАНАЛ УДАЛЁННЫЙ БАНКОВСКИЙ

КУБ — экономичный формат мини-офисов, позволяющий развернуть масштабную банковскую инфраструктуру при небольших финансовых затратах.

Банковская система страны в своём развитии заметно отстаёт от потребностей рынка. Банковская сеть почти из 31 тысяч пунктов банковского обслуживания на всю Российскую Федерацию (по состоянию на конец 2018 года) явно недостаточна, и поэтому степень охвата населения банковскими услугами далека от европейской.

Причины сложившейся ситуации в том, что создание даже одного классического банковского отделения — достаточно затратное мероприятие. Это приобретение помещения, серьёзные инвестиции в охрану и системы безопасности, в дорогостоящее оборудование и квалифицированный персонал.

Поэтому система электронных платежей «КиберПлат» (CyberPlat®) разработала и предлагает банкам и торговому ритейлу законченное полнофункциональное решение, позволяющее быстро развернуть продажи финансовых продуктов и приём платежей, — КУБ. Перенос банковских операций за пределы банковских отделений стал возможен благодаря изменению законодательства и новым нормам в сфере приёма платежей, вступившим в силу с 1 января 2010 года.

Как было раньше?

До изменения законодательства можно было принимать платежи по агентской схеме в пользу тех провайдеров, с которыми заключены договоры и организовано информационно-технологическое взаимодействие между учётными системами (разработаны шлюзы).

После изменения законодательства стало можно:

- принимать платежи по агентской схеме в пользу тех провайдеров, к учётным системам которых имеются шлюзы;
- принимать платежи по шаблону (банковский провайдер);
- принимать любые платежи:
 - за товары;
 - за услуги;



- налоговые;
- на пополнение банковских счетов физических лиц.

А также заключить договор в качестве банковского платёжного агента от имени принципала на заключение договоров в сферах:

- банковских услуг (включая договор на открытие счетов);
- страховых услуг (включая оформление полиса);
- услуг связи (включая продажу контрактов).

При этом операционист в качестве агента банка идентифицирует клиента и определяет шаблон платежа, а сама банковская операция, например денежный перевод, совершается через банковский терминал.

Техническая комплектация мини-офиса КУБ:

- настенный генератор штрих-кодов;
- cash-in-терминал;
- рабочее место кассира:
 - лэптоп с выходом в интернет;
 - устройство для печати чеков ККМ;
 - сканер и принтер формата А4, сканер штрих-кодов;
 - устройство для проверки подлинности купюр, сейф.



КАКИЕ ОПЕРАЦИИ МОЖНО ПРОВОДИТЬ В МИНИ-ОФИСЕ КУБ?

Продавать финансовые продукты:

-  Открытие банковских счетов
-  Банковские карты
-  Депозиты
-  Кредитование
-  Страхование
-  Другие

Принимать платежи:

-  Квартплата и коммунальные платежи
-  Оплата штрафов и пошлин
-  Фиксированная и сотовая связь
-  Интернет и коммерческое ТВ
-  Другие платежи от физических лиц
-  Денежные переводы

ВОЗМОЖНЫЕ ФОРМАТЫ РАБОТЫ КУБА

В зависимости от количества и качества подготовки кассиров-операционистов возможно несколько вариантов работы с клиентами:

	Скоростной	Сервисный	Комбинированный
Уровень грамотности кассиров	Низкая квалификация	Высокая квалификация	Средняя квалификация
Число операционистов	2	1	1
Сдача	Строго на телефон или счет в банке	По желанию клиента	По желанию клиента
Сервисы	Только ЖКХ, сотовая связь, интернет	Все виды платежей с упором на страхование, контракты, связи, кредиты и депозиты	Все виды
	Возможна установка «двойного» КУБа: одна «продвинутая» операционистка все объясняет, одна операционистка с низкой квалификацией принимает платежи быстро		

В зависимости от места установки КУБа нагрузка на операциониста и терминал может быть разной

В холле технического университета, как мы предполагаем, соотношение платежей кассир/терминал будет 1/2, поскольку плательщиками будут молодые, технически грамотные студенты.

В холле учреждения социального обеспечения, по нашим расчётам, соотношение платежей кассир/терминал будет 7/1, поскольку плательщиками являются пожилые люди, не доверяющие технике и склонные к ошибкам.

Квартплату и коммунальные платежи, как показывает практика, клиенты также предпочитают вносить через кассира.

Платёжи в основном принимаются «без сдачи» — она просто зачисляется на оплату других услуг, как правило, сотовой связи. Количество клиентов КУБа больше в 3–4 раза, а средний платёж больше в 2–3 раза по сравнению с терминалом, расположенным в этой же зоне.

ПОЧЕМУ СИСТЕМА КУБ ЭФФЕКТИВНЕЕ И ДЕШЕВЛЕ БАНКОВСКИХ ОТДЕЛЕНИЙ

- КУБ не принадлежит банку и не подпадает под требования ВНП-001-01 по уровню защищённости.
- Периодическая инкассация (рекомендуется при накоплении в кассе 30 тысяч рублей) в cash-in-терминал, принадлежащий банку, позволяет снизить кассовые риски и оптимизировать процесс инкассации по времени.
- Почти любую банковскую операцию может оформить кассир, работающий по совместительству, деньги вносятся в cash-in-терминал, принадлежащий банку.

- Возможен приём платежей на сумму свыше 15 тысяч рублей, требующих идентификации.
- Ввод данных по штрих-коду:
 - намного быстрее;
 - исключает ошибки речи, слуха и ввода данных.
- «КиберСдача» на телефон:
 - экономия времени;
 - проще, чем сдача монетами;
 - точнее (нет риска ошибиться со сдачей);
 - приносит доход с суммы сдачи.

КАКОВА СТОИМОСТЬ РАЗМЕЩЕНИЯ МИНИ-ОФИСОВ КУБ

- Полный комплект оборудования — \$3500.
- Перемещение в другое место — \$100.
- Для полного охвата ритейлового рынка, к примеру, Москвы необходимо 4–5 тысяч офисов формата КУБ.
- Это потребует менее \$20 миллионов инвестиций.

ВАЖНО!

Размещать мини-офисы следует в местах высокой проходимости!

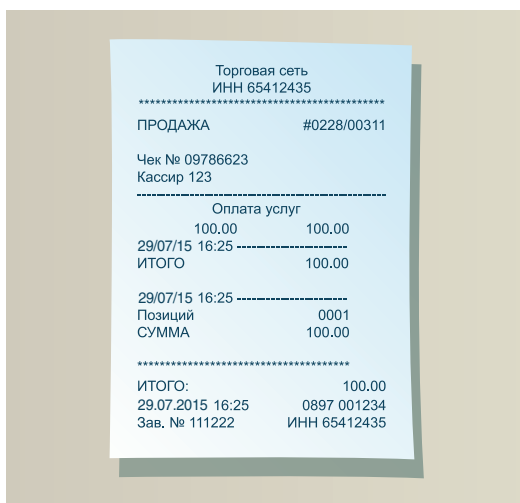
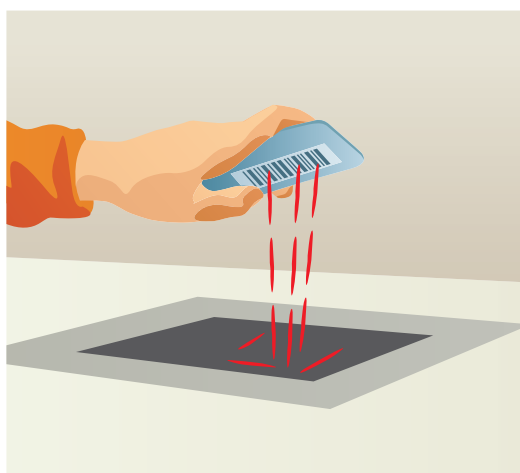
ПАКЕТ ПОСТАВКИ КУБ

- Методические материалы:
 - инструкция кассира КУБа;
 - инструкция менеджера КУБов.
- Программное обеспечение по приёму платежей через Кабинет агента:
 - в пользу провайдеров, к учётным системам которых имеются шлюзы;
 - в пользу банковских провайдеров (в том числе самостоятельное формирование учётных записей в системе);
 - по свободным реквизитам.
- ИСДП — денежные переводы по трём системам.
- Интегратор POS-кредитов.
- Интегратор продажи контрактов на использование пластиковых карт.
- Интегратор продажи контрактов связи.
- Интегратор страховых контрактов.

КАК ЭТО РАБОТАЕТ?

Получив карту «КиберСдача» со штрих-кодом, соответствующим номеру сотового телефона, лицевого счёта или номера договора с провайдером услуг, клиент может использовать её для регулярных платежей в мини-офисе КУБа.

- Клиент подходит к кассиру, называет услугу, которую хочет получить (пополнение счёта у оператора сотовой связи, плата за квартиру или коммунальные услуги, погашение кредита и т.п.).



- При наличии карты «КиберСдача» со штрих-кодом кассир считывает штрихкод сканером. Необходимые дополнительные поля в специализированном ПО (например, сумма платежа) заполняются кассиром со слов клиента.
- После приёма денег кассиром выполняются следующие операции:
 - вводится дополнительная информация в экранной форме специализированного ПО;
 - отправляется запрос на наличие такого номера счёта у провайдера;
 - получается разрешение на осуществление операции;
 - отправляется запрос на выполнение операции;
 - получается ответ от системы «КиберПлат» (CyberPlat®) об успешном завершении операции;
 - распечатывается кассовый чек и передаётся клиенту.

Для простых услуг, таких как приём оплаты сотовой связи, полный цикл обслуживания не превышает 15 секунд, включая передачу клиенту кассового чека!

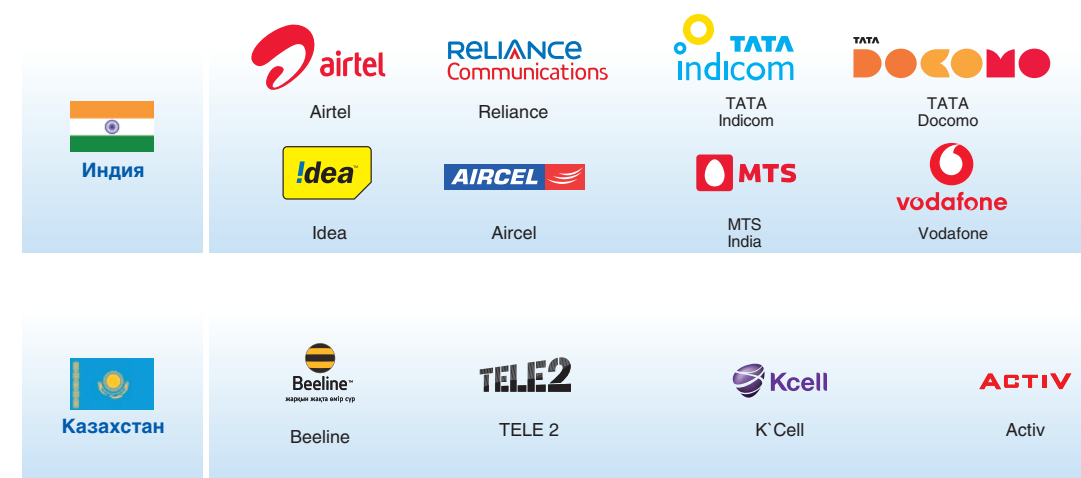
- В случае отсутствия карты «КиберСдача» со штрих-кодом кассир выдает её после платежа.
- Для ускорения процесса обслуживания сдача клиенту сразу зачисляется, например, на абонентский счёт у оператора сотовой связи.

INTERNATIONAL TOP-UP: МЕЖДУНАРОДНЫЕ ОПЕРАТОРЫ И ТРАНСГРАНИЧНЫЕ ПЛАТЕЖИ

Абоненты за рубежом могут оплачивать мобильную связь с помощью международной системы электронных платежей «КиберПлат» (CyberPlat®).

Во многих зарубежных странах существует развитая сеть точек приёма платежей, расположенная на предприятиях торговли и сервиса и подключённая к системе «КиберПлат» (CyberPlat®). Часть этих стран объединена уникальной системой трансграничных платежей. Жители Казахстана, Индии и России, входящих в систему, могут на территории любой из этих стран легко и быстро пополнить свои счета у различных провайдеров, внося платёж в местной национальной валюте.

Разработанная компанией «КиберПлат» (CyberPlat®) инфраструктура трансграничных платежей создаёт комфортные условия для населения различных стран. Этот сервис особенно востребован абонентами операторов мобильной связи, проживающими на сопредельных территориях или часто путешествующими.



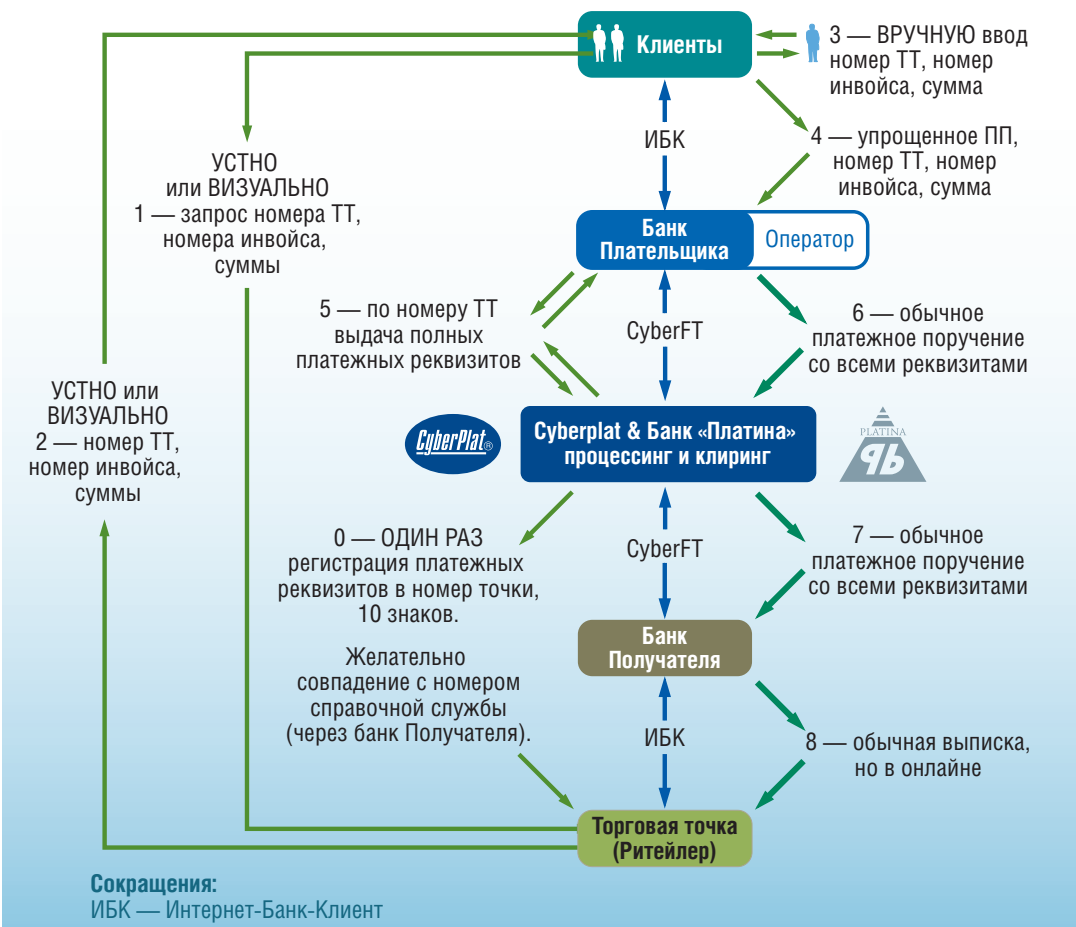
РЕШЕНИЯ В СФЕРЕ МОБИЛЬНОЙ КОММЕРЦИИ

CYBERPAY

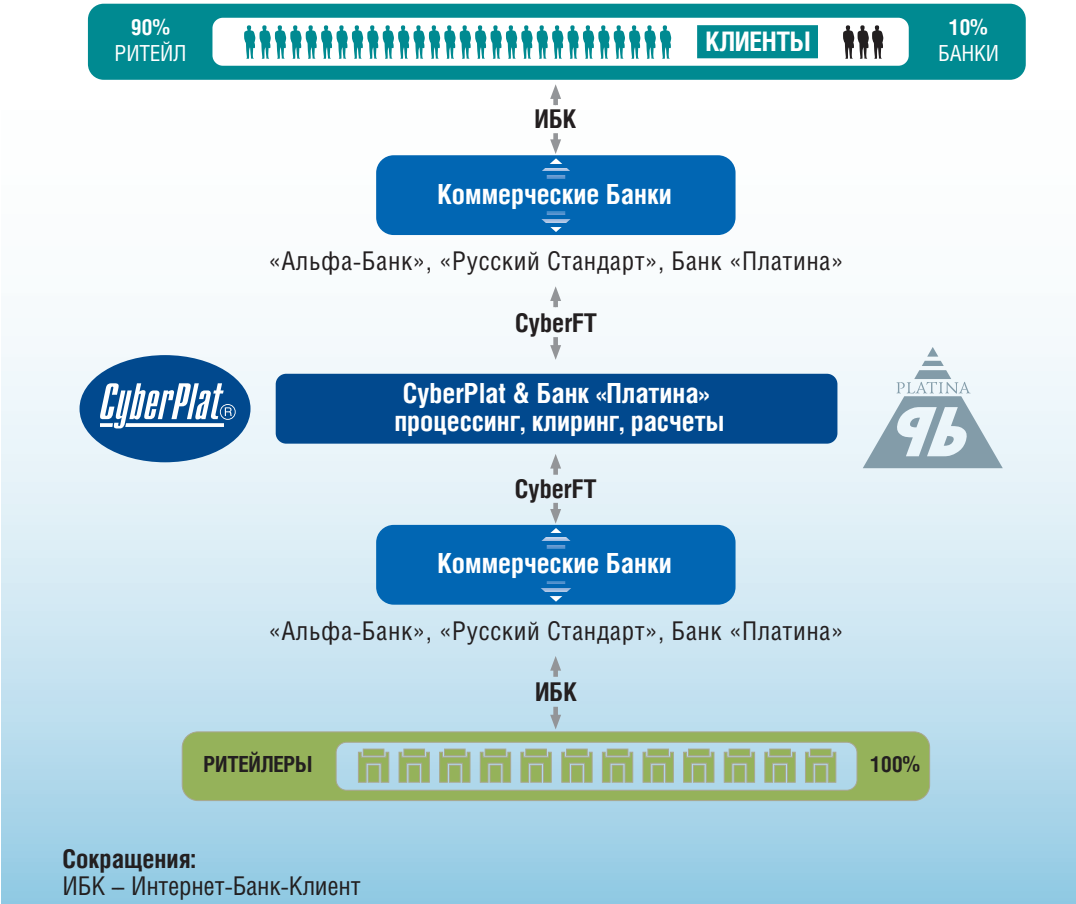
CyberPay — это решение «КиберПлат» (CyberPlat®), позволяющее с помощью специального приложения на мобильном телефоне осуществлять платежи за покупки в торговых предприятиях, предварительно зарегистрированных в системе электронных платежей. Списание средств происходит с расчётного счёта в банке плательщика. Данная технология внедрена и апробирована в пилотном проекте совместно с сетью салонов связи «Ноу-Хау».

Особенности решения CyberPay

- Основано на электронном документообороте стандартных платёжных поручений в соответствии с действующим законодательством.
- Использует платформу CyberFT для оперативного обмена платёжными поручениями.



Технология CyberPay



Общая схема CyberPay

- Обеспечивает высокую оперативность (1 секунда на передачу платёжного поручения от банка плательщика до банка получателя).
- Обеспечивает информационную безопасность на уровне «банк плательщика — банк получателя» по технологии «КиберПлат» (CyberPlat®), на уровнях «плательщик — банк плательщика» и «получатель — банк получателя» — в соответствии с имеющимися решениями банков.
- Полностью открытые форматы, протоколы и шлюзы — в качестве ИБКБ может быть использовано не только решение «КиберПлат» (CyberPlat®), но и собственное решение банка-партнёра.

Технология CyberPay чрезвычайно выгодна предприятиям ритейла по следующим причинам:

- Снижение необходимой суммы заёмных средств за счёт ускорения оборота. При использовании технологии CyberPay происходит мгновенное зачисление полученной суммы на банковский счёт, в отличие как от оплаты по банковским картам (трое суток), так и от оплаты наличными (сутки на инкассацию и пересчёт).
- Меньшая комиссия по сравнению с эквайрингом пластиковых карт.
- Привлечение новых «высокотехнологичных» покупателей.

- Традиционные преимущества безналичных платежей по сравнению с оплатой наличными:
 - избавление от процесса выдачи сдачи и расходов на доставку монет из банка;
 - отсутствие затрат на инкассацию;
 - сокращение времени обслуживания покупателя на кассе;
 - упрощение кассовой документации;
 - рост среднего чека за счёт спонтанных покупок.

ТЕХНОЛОГИЯ CYBERDEN — УНИКАЛЬНЫЙ ИНСТРУМЕНТ МОБИЛЬНОЙ КОММЕРЦИИ

CyberDeN—это система электронных платежей нового поколения, превосходящая VISA. Оптимизированная технология мобильных платежей разработана группой ведущих специалистов «КиберПлат» (CyberPlat®), МТС, Билайн, МегаФон, Сбербанк России, Банка Русский Стандарт.

Что такое мобильные платежи

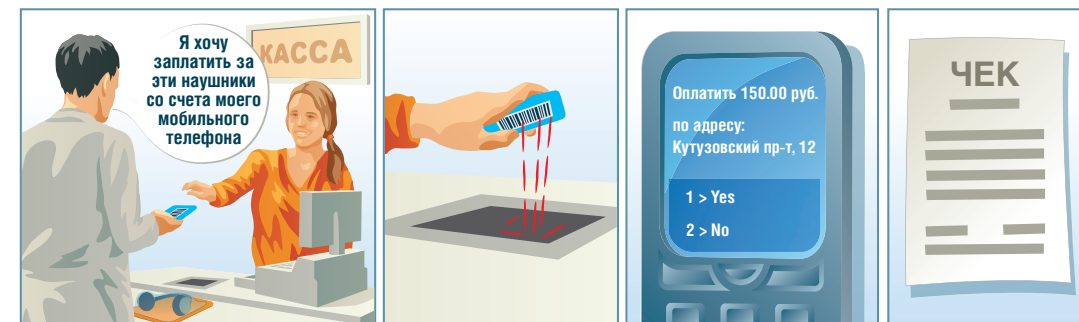
Это новый способ платежей на предприятиях розничной торговли, позволяющий списывать деньги за покупку либо с лицевого счёта оператора сотовой связи, либо с банковского счёта плательщика. Идентификатором лицевого счёта абонента является уникальный для каждого номера сотового телефона штрих-код. Возможность оплаты с лицевого счёта абонента позволяет осуществлять покупки в ситуации, когда с собой нет ни денег, ни банковской карты.

Почему это важно для операторов сотовой связи и банков

Участие в проекте по внедрению технологии мобильной коммерции CyberDeN позволяет сотовым операторам и банкам увеличить и цементировать остатки на счетах физических лиц, предназначенные для совершения покупок. Общий объём денежных средств в виде банковских вкладов на конец 2018 года составлял 28,5 триллионов рублей (примерно \$409 миллиардов). За счёт ожидаемого быстрого роста сектора мобильной коммерции его участники смогут получить долю в 30% на рынке вкладов физических лиц до востребования, то есть до \$123 миллиардов. Понятно, что это весьма привлекательно как для сотовых операторов, так и для банков.

Как это выглядит со стороны клиента

В момент оплаты продавец сканирует штрих-код, наклеенный на мобильный телефон или специальную карту, а на мобильный телефон клиента приходит USSD-запрос на подтверждение покупки с указанием суммы и адреса места покупки. Клиент акцептует платёж, после чего продавец получает подтверждение от системы электронных платежей о перечислении средств в режиме онлайн, печатает чек и отдаёт товар.

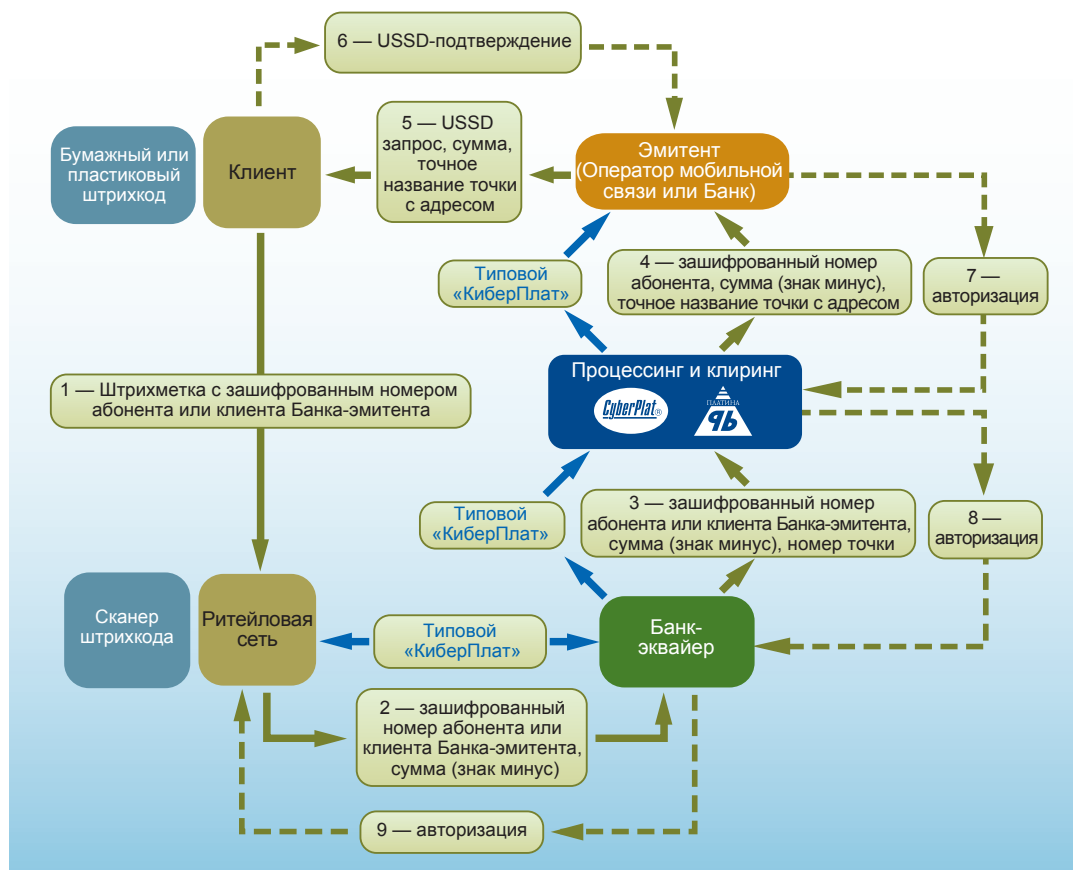


КАК ЭТО РАБОТАЕТ

1. В момент оплаты продавец сканирует штрих-код, наклеенный на телефон абонента или специальную карту.
2. Программное обеспечение кассы формирует и передаёт по технологии «КиберПлат» (CyberPlat®) запрос, содержащий зашифрованный номер абонента или клиента банка, сумму и номер точки на подтверждение платежа в банк-эквайер.
3. Банк-эквайер передаёт по технологии «КиберПлат» (CyberPlat®) запрос в систему электронных платежей «КиберПлат» (CyberPlat®).
4. Система «КиберПлат» (CyberPlat®) по коду торговой точки определяет её адрес.
5. Система электронных платежей «КиберПлат» (CyberPlat®) передаёт запрос банку-эмитенту или оператору сотовой связи (эмитенту штрих-кодовой метки). Запрос содержит зашифрованный номер абонента или клиента банка, сумму, адрес и номер торговой точки.
6. Оператор сотовой связи, если средств абонента на лицевом счёте достаточно, отправляет абоненту зашифрованный или нешифрованный USSD-запрос, содержащий сумму и точный адрес торговой точки.
7. Абонент акцептует USSD-запрос либо отказывается от платежа.
8. Оператор сотовой связи (в случае если он является эмитентом штрих-кодовой метки) передаёт системе электронных платежей «КиберПлат» (CyberPlat®) авторизацию платежа.

или

1. Банк-эмитент (в случае если он является эмитентом штрих-кодовой метки):
 - при достаточности средств клиента на расчётном счёте отправляет системе электронных платежей «КиберПлат» (CyberPlat®) предварительный акцепт (подтверждает принципиальную возможность платежа), номер телефона клиента и код обслуживающего оператора сотовой связи;
 - «КиберПлат» (CyberPlat®) через собственный USSD-концентратор передаёт клиенту зашифрованный или нешифрованный USSD-запрос, содержащий сумму и точный адрес торговой точки;
 - абонент акцептует USSD-запрос либо отказывается от платежа;



КЛЮЧЕВОЕ ПРЕИМУЩЕСТВО — ИСПОЛЬЗОВАНИЕ ШТРИХ-КОДА



Штрих-код считывается и идентифицируется со специальной метки, наклеенной на карточке или на обратной стороне мобильного телефона. Штрих-код можно распечатать через информационный киоск — принтер штрих-кодов.

На совершение запроса уходит всего 3 секунды, на получение ответа — тоже 3 секунды!

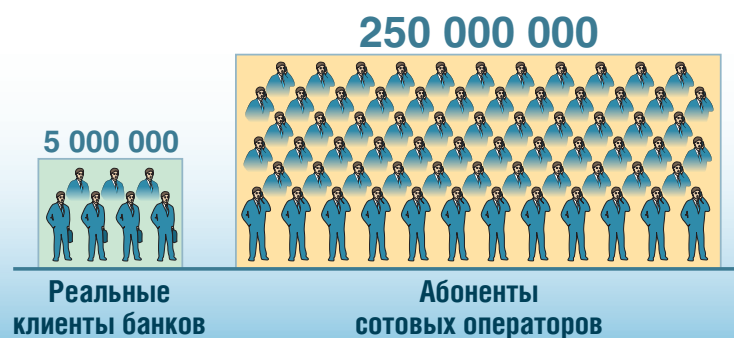
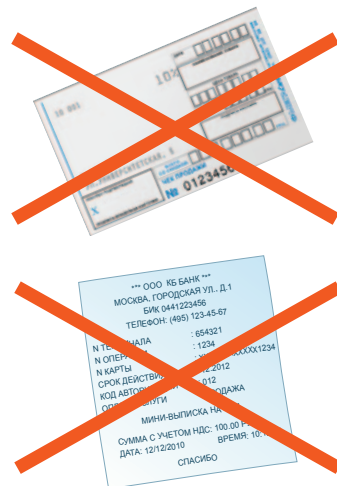
ОТЛИЧИЯ ТЕХНОЛОГИИ CYBERDEN ОТ КЛАССИЧЕСКОЙ ТЕХНОЛОГИИ VISA

1. Физически отсутствует пластиковая карта. Она заменяется нестираемой наклейкой со штрих-кодом, содержащим информацию о номере счёта клиента и его эмитенте (банк или оператор сотовой связи).



2. Таких одинаковых наклеек, в отличие от карты, можно иметь сколько угодно (например, одна на телефоне, другая — на сберегательной книжке, третья — на бумажнике и т.п.).
3. Отсутствует бумажный документооборот, поскольку вместо подписания слипа происходит подтверждение USSD-запроса. Резко упрощается разбор конфликтных ситуаций, снижаются затраты на претензионную работу.

4. Суммы платежей небольшие, основная часть транзакций — до \$30 (максимум \$50). Однако при этом охватывается весь торговый ритейл (49% всего оборота домохозяйств), что составляет примерно \$330 миллиардов в год.
5. Списание средств (cash-out transaction) возможно не только с банковских счетов, но и с лицевых счетов абонентов у операторов сотовой связи (и шире, с клиентских счетов любой организации, получившей доверенность от банка на сбор платёжных поручений с клиентов в соответствии с ФЗ № 121).
6. Списание со счёта клиента/зачисление торговой точке для ритейлера дешевле в 2 раза, чем через системы VISA или MasterCard, и происходит в режиме онлайн.



- Комиссия Interchange fee для участников системы электронных платежей фиксирована и составляет \$0,01.
 - Себестоимость списания в биллинге оператора — 2 цента против 10 в системе «опердень» банка.
7. Возможно зачисление денег как на указанные счета в банки (cash-in transaction), так и на лицевые счета абонентов у операторов связи (top up). Прежде всего, ожидается использование данной возможности для наличных платежей типа «сдача на телефон или на счёт в банке».



ВЫГОДЫ ОТ ИСПОЛЬЗОВАНИЯ СЕРВИСА «МОБИЛЬНЫЕ ПЛАТЕЖИ»



Для клиентов

- Новый современный платёжный инструмент.
- Доверие к операторам связи выше, чем к банкам.
- При отсутствии наличных средств всегда можно оплатить товары и услуги непосредственно со своего лицевого счёта, используя мобильный телефон.
- Скорость покупки выше, чем при покупке по пластиковой карточке.
- Безбумажный документооборот.
- Безопасность — списание средств не происходит с лицевого счёта без подтверждения операции самим абонентом.
- Сеть для пополнения лицевого счёта огромна (несравнима с количеством офисов и банкоматов отдельного банка).

Для предприятий ритейла

- Низкая стоимость приёма платежей (от 0,7 до 1%).
- Мгновенное зачисление средств на счёт в банке.
- Отсутствие необходимости замены эксплуатируемого оборудования.
- Скорость:
 - вся операция занимает не более 6 секунд (3 секунды от торговой точки до покупателя и 3 секунды — обратно);
 - выше скорости оплаты с использованием пластиковой карточки и снижение расходов на приём платежей;
 - позволяет начать приём платежей в дискаунтерах и супермаркетах.
- Увеличение объёма продаж за счёт продаж лицам, у которых кончились наличные и которые «забыли дома» карточку (рост числа платёжных инструментов у покупателя).
- Продажи в основном недорогих и высокомаржинальных товаров.
- Снижение количества возможных конфликтных ситуаций.
- Снижение рисков работы с наличными.



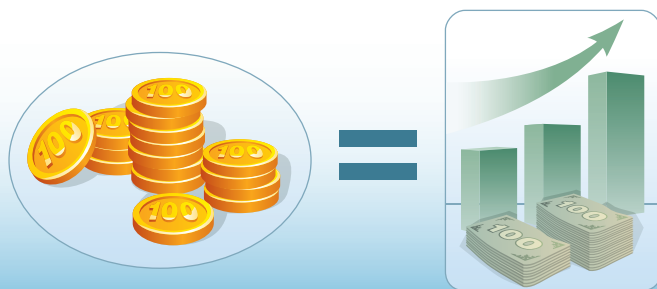
Для операторов сотовой связи

- Рост остатков на лицевых счетах абонентов увеличит пассив компании, по оценкам значительно — в перспективе больше чем на \$1 миллиард (для компаний уровня «большой тройки»).
- Отсутствие инвестиций.
- Высокая скорость внедрения.
- Опережение конкурентов во внедрении реальной мобильной коммерции.
- Создание имиджа супертехнологичной компании при минимальных затратах.
- Стимуляция торговых точек на приём платежей за сотовую связь и реализация программы «сдача на телефон или счёт в банке».
- При использовании операции со считыванием штрих-кода:
 - ошибки сводятся к минимуму и, как следствие, снижаются затраты на отмены и корректировки платежей;
 - ускоряется время операции, что позволит торговым сетям:
 - уменьшить расходы на приём платежей,
 - ускорить время приёма одного платежа,
 - начать приём платежей в дискаунтерах и супермаркетах.



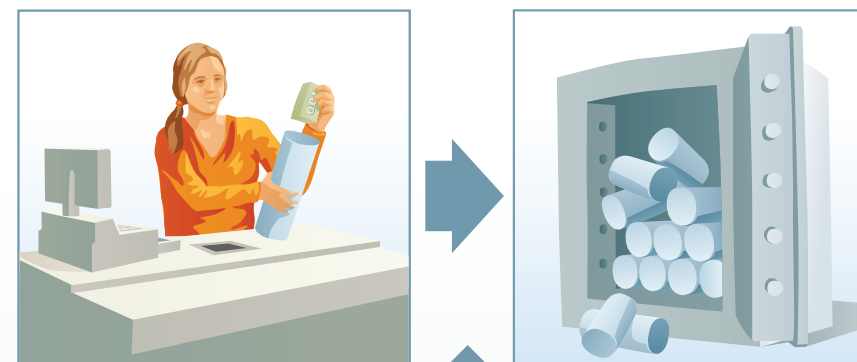
Для банков-эквайеров

- Более плотная «привязка» клиентов-ритейлеров к банку.
- Повышение обеспеченности кредитов, выдаваемых ритейлерам.
- Получение дополнительных эквайринговых доходов и конкурентных преимуществ.
- Возможность начать работу с торговыми предприятиями, традиционно не принимающими карты к оплате из-за высокой комиссии.
- Вывод на рынок продукта, способного составить конкуренцию международным платёжным системам.
- Стимуляция торговых точек на приём платежей за сотовую связь и реализация программы «сдача на телефон или счёт в банке».
- Опережение конкурентов во внедрении реальной «мобильной коммерции».
- Создание имиджа супертехнологичного банка.



ОНЛАЙН-ИНКАССАЦИЯ

Текущая технология инкассации крупных супер- и гипермаркетов устарела и недостаточно автоматизирована, что влечёт за собой большие издержки и повышенные риски при осуществлении процессов сдачи, перевозки, пересчёта и зачисления инкассированной наличности.



1. Упаковка денег в специальную тару

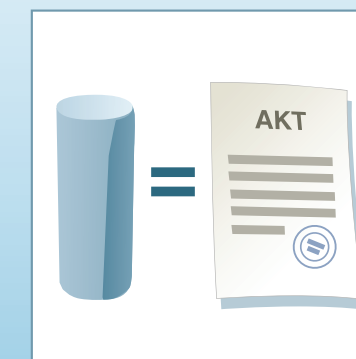
2. Складирование в сейфе в ожидании инкассации



3. Изъятие денег инкассаторами и доставка в банк



4. Пересчет доставленных денег в банке



Каждый этап сопровождается оформлением соответствующих документов

На сегодняшний день зачисление средств на расчётный счёт ритейлера после инкассации в торговой точке может занимать до трех дней. Кроме того, существующая система инкассации не избавлена от рисков мошенничества при передаче и хранении наличных денежных средств, что приводит к дополнительным затратам в сфере охраны и безопасности.

Специалистами «КиберПлат» (CyberPlat®) разработана технология онлайн-инкассации, которая позволяет оптимизировать этот процесс, а также значительно снизить издержки, риски и сроки этой процедуры.



Это технология принципиально новых «электронных кассиров» — специализированных терминалов, способных принимать и пересчитывать пачки наличности. С помощью технологий «КиберПлат» (CyberPlat®) денежные средства, внесённые в такой терминал кассирами торговых сетей, в режиме реального времени окажутся на расчётном счёте ритейлера в расчётном банке.

КАК ЭТО РАБОТАЕТ

Инкассирующий терминал, размещённый в ритейловой точке, обеспечивает автоматизацию учёта инкассируемых купюр, их защищённое хранение, авторизацию служебных пользователей системы, передачу информации об операциях и транзакциях в процессинговый центр «КиберПлат» (CyberPlat®).

Каждая ритейловая точка имеет регистрационный код в системе «КиберПлат» (CyberPlat®), а на каждом инкассационном терминале устанавливается неизвлекаемый ключ ЭП (не менее 2048 бит).

Купюроприёмник инкассационного терминала оборудован считывателем номера купюр.

Функционал инкассационного терминала:

- идентификация персонала, работающего с устройством, обеспечение доступа;
- пачечный/покупюрный приём банкнот;
- определение номинала и подлинности банкнот (валидация);
- подсчёт суммы депонированных банкнот;
- хранение банкнот;
- обработка, хранение и передача информации в «КиберПлат» (CyberPlat®), для дальнейшей передачи в инкассирующий и расчётный банк.

Важно: при каждой транзакции, до выполнения процедур работы с терминалом, ответственные сотрудники (главный кассир, кассир или инкассатор) авторизуются в системе и вводят PIN-код.

Кроме того, при печати чеков и актов на документах печатается значение ЭП.



ОБЩАЯ СХЕМА ИНКАССАЦИИ РИТЕЙЛОВОЙ ТОЧКИ С ИСПОЛЬЗОВАНИЕМ ИНКАССАЦИОННОГО ТЕРМИНАЛА

1. Пройдя процедуру авторизации, сотрудники торговой точки вносят выручку в терминал.
2. Терминал производит автоматический пересчёт денежных средств. Терминал передаёт информацию о внесённой сумме в процессинговый центр «КиберПлат».
3. Процессинговый центр «КиберПлат» ретранслирует полученную информацию о внесённой сумме денежных средств в расчётный банк для зачисления на счёт клиента.
4. Процессинговый центр «КиберПлат» выводит на печать комплект документов для клиентов, содержащий информацию о внесённой сумме.
5. Клиент получает на руки распечатанный комплект документов, подтверждающий проведение транзакции.

ОБЩАЯ СХЕМА ИНКАССАЦИИ ТЕРМИНАЛА

1. Инкассатор, пройдя процедуру авторизации, получает доступ к работе на терминале. Он производит изъятие из терминала кассет с денежной наличностью и устанавливает комплект новых кассет для дальнейшей работы терминала.
2. Факт проведения инкассации фиксируется в процессинговом центре «КиберПлат». Также в процессинговый центр передаётся информация об общей инкассированной сумме.
3. Процессинговый центр «КиберПлат» выводит на печать комплект документов для инкассаторов, содержащий информацию об общей сумме денежной наличности, извлечённой из терминала.



ДОПОЛНИТЕЛЬНЫЕ СЕРВИСЫ ДЛЯ ПАРТНЁРОВ «КИБЕРПЛАТ» (CYBERPLAT®)

4. Инкассатор получает на руки распечатанный комплект документов, который содержит информацию об общей сумме наличных, извлечённых из терминала, и одновременно выступает в роли сопроводительных документов при перевозке кассет с деньгами в банк.
5. Процессинговый центр «КиберПлат» ретранслирует информацию о факте проведения инкассации, включающую сведения о сумме инкассированной денежной наличности.

Процесс инкассации состоит из двух этапов: внесение наличных денег в инкассационный терминал и инкассация терминала. На первом этапе сотрудники ритейловой точки вносят деньги в терминал — при этом данные о внесённой сумме (включая номера купюр) передаются в «КиберПлат» (CyberPlat®). После обработки данных «КиберПлат» (CyberPlat®) передаёт информацию о внесении денег в расчётный банк ритейловой точки, который зачисляет внесённую сумму на расчётный счёт ритейлера.

Все операции выполняются в режиме онлайн, что позволяет зачислить деньги на счёт ритейлера в течение нескольких секунд после завершения процедуры внесения наличности в терминал.

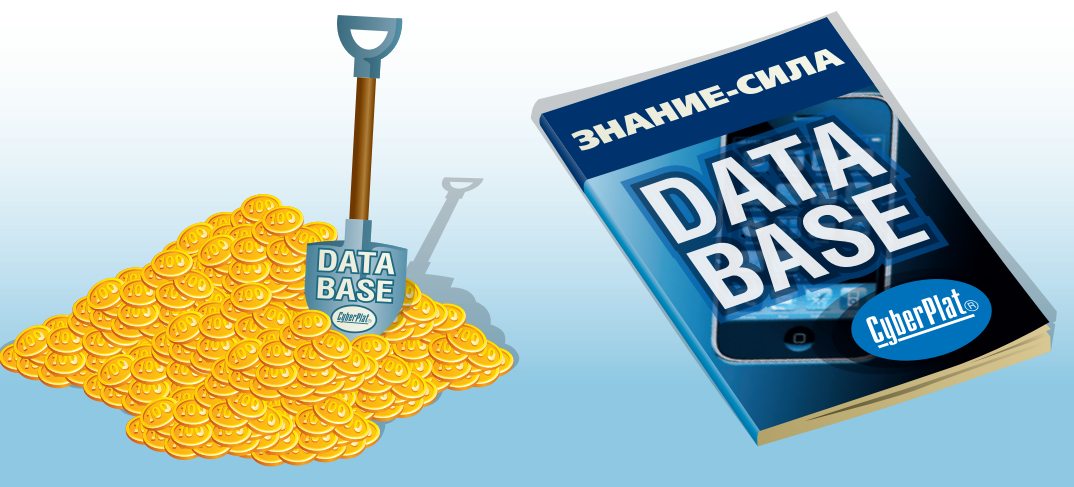
На следующем этапе инкассатор и расчётный банк проводят процедуру инкассации терминала. После пересчёта расчётный банк сообщает инкассированную сумму в «КиберПлат» (CyberPlat®) для сверки.

Преимущества технологии онлайн-инкассации

- Процесс сдачи и верификации выручки для кассира занимает от 2 до 10 минут.
- Нет необходимости пересчитывать купюры в каждом тубусе.
- Риск воровства при пересчёте резко снижается при считывании и хранении номеров каждой банкноты.

Расчёты показывают, что внедрение такой технологии способно охватить до 70% рынка инкассации супер- и гипермаркетов и до 40% рынка более мелких магазинов в торговых центрах.

СКОРИНГ ПО НОМЕРУ ТЕЛЕФОНА

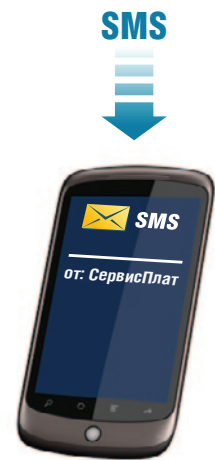


На конец 2018 года база данных о клиентах системы электронных платежей «КиберПлат» (CyberPlat®) содержала более 12 миллиардов записей, содержащих данные «дата — время — номер телефона — сумма — место платежа».

Результаты анализа этой базы данных могут представлять большой интерес для бюро кредитных историй и банков. Подобный анализ может быть проведён в целях проверки платёжеспособности клиентов и оценке рисков кредитования.

Использование скоринга по номеру телефона позволит кредитному бюро или банку повысить точность и оперативность предоставляемого или собственного кредитного скоринга, а также сократить издержки и повысить качество предоставляемых услуг.

ЦЕЛЕВОЕ SMS-ИНФОРМИРОВАНИЕ*



Еще одна возможность, предоставляемая системой электронных платежей «КиберПлат» (CyberPlat®) своим партнёрам — это целевое информирование клиентов о новых возможностях, продуктах и услугах при помощи SMS-сообщений.

С помощью этой системы клиенты, которые платят через пункты приёма платежей, принадлежащие конкретным агентам, информируются, к примеру, о новых видах платежей и новых провайдерах — региональных или местных поставщиках коммунальных услуг, о возможности приобретения виртуальных банковских карт или приёме денежных переводов.

* Услуга SMS-информирования предоставляется только в случае получения согласия от потребителя.

Сервис целевого SMS-информирования может быть также предложен партнёрам агентов «КиберПлат» (CyberPlat®) — к примеру, торговым предприятиям или сетям, где расположены терминалы или пункты приёма платежей агентов системы электронных платежей. Ритейлеры могут таким образом рекламировать свои товары, услуги или маркетинговые акции. Агентам же это помогает укреплять взаимоотношения со своими деловыми партнёрами.

При разработке конкретной кампании SMS-информирования устанавливаются критерии выбора получателей — к примеру, они могут направляться только тем, кто платит за коммунальные услуги, или только тем, кто заплатил более 300 рублей, или только плательщикам за сотовую связь и т.п.

Данный сервис представляет собой эффективный маркетинговый инструмент и позволяет агентам повышать посещаемость их точек приёма платежей, увеличивать их обороты и тем самым повышать эффективность бизнеса в целом.

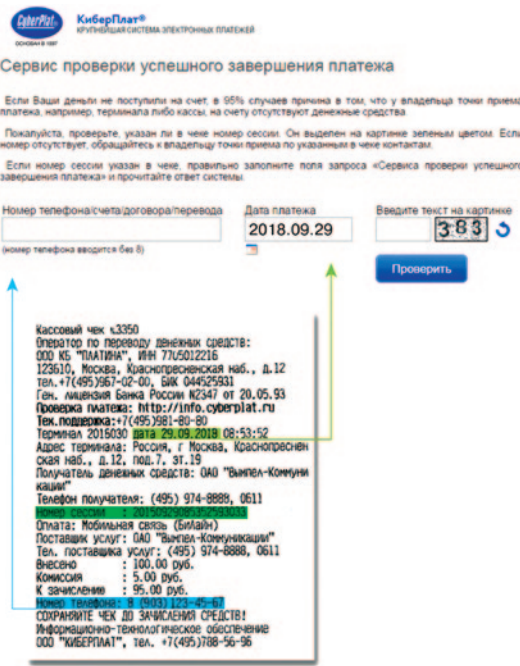
МОНИТОРИНГ ТРАНЗАКЦИЙ В РЕЖИМЕ ОНЛАЙН

Для удобства клиентов, осуществляющих платежи через систему «КиберПлат» (CyberPlat®), а также агентов системы электронных платежей разработан специальный веб-сервис проверки состояния произведенного платежа (info.cyberplat.ru).

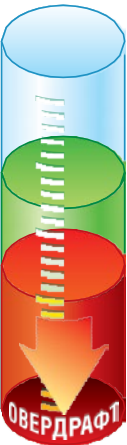
Клиент (или агент) вводит в специальные поля номер сотового телефона (или номер договора — в случае платежей не в пользу оператора сотовой связи), дату осуществления платежа и проверочный код для защиты от сетевых роботов.

После этого пользователь получает информацию о статусе платежа: «прошел», «не найден», «отправлен на обработку провайдеру», «отменён в системе «КиберПлат».

Далее, в зависимости от статуса платежа, клиенту рекомендуются те или иные действия — к примеру, обратиться к провайдеру, либо к агенту, через которого принят платёж, либо в службу клиентской поддержки «КиберПлат» (CyberPlat®). Такой сервис предоставляет дополнительные удобства для клиентов и агентов и значительно облегчает претензионную работу с плательщиками.



ОНЛАЙН-КРЕДИТОВАНИЕ



Счет агента

Специалистами «КиберПлат» (CyberPlat®) разработан сервис автоматического кредитования в Банке «Платина» (расчётном банке системы электронных платежей) — под комиссию от принятых платежей.

Данный сервис обеспечивает более высокую стабильность работы сетей приёма платежей партнёров «КиберПлат» (CyberPlat®) в выходные и праздничные дни, поскольку снижает потребность в экстренном перечислении денежных средств в Банк «Платина» для обеспечения расчётов по принятым платежам.

Программа онлайн-кредитования предоставляет возможность автоматического кредитования в режиме овердрафта на сумму начисленных комиссий за уже принятые платежи. Для участия в программе партнёр должен иметь расчётный счёт в Банке «Платина» и подписать договор на предоставление овердрафта.

ПРОДУКТЫ B2C

PLAT.RU — «ПЛАТЁЖНАЯ КНИЖКА КИБЕРПЛАТ»

Сервис Plat.ru — «Платёжная книжка КиберПлат», разработанный специалистами «КиберПлат» (CyberPlat®) и Банка «Платина», успешно эксплуатируется несколько лет.

Возможности для клиентов

Клиентом этого удобного сервиса может стать любой человек, зарегистрировавший свою персональную «Платёжную книжку» на сайте plat.ru или через терминалы и кассиров торговых точек партнёров системы электронных платежей «КиберПлат» (CyberPlat®). Пополнив баланс своей «Платёжной книжки», пользователь получает возможность через веб-интерфейс совершать платежи в адрес широкого круга операторов услуг (всего более 8 тысяч) — сотовой и проводной связи, кабельного и спутникового телевидения, интернет-провайдеров, поставщиков коммунальных услуг, оплачивать госуслуги и др.

Пополнять баланс «Платёжной книжки» можно через терминалы и кассы торговых точек тех партнёров «КиберПлат» (CyberPlat®), которые подключены к сервису. За пополнение баланса «Платёжной книжки» предусмотрена комиссия с клиента в пользу агента, через которого осуществляется операция. Без дополнительной комиссии пополнение баланса «Платёжной книжки» возможно через терминалы Банка «Платина» (их адреса — на сайте www.platina.ru).

«Платёжная книжка» сохраняет реквизиты постоянных платежей, что позволяет проводить операции пополнения лицевого счета или погашения



накопившейся задолженности в считанные секунды. Сохранение истории проводимых операций позволит не только пользователям контролировать текущие расходы, но и планировать личный бюджет.

Важным преимуществом нового сервиса является возможность регистрации в системе новых получателей платежей — к примеру, местных операторов сотовой связи, кабельного телевидения или жилищно-коммунальных предприятий. Таким образом, пользователь «Платёжной книжки» получает уникальный сервис платежей «из одного окна» в любое время суток семь дней в неделю, в том числе в случае возникновения экстренной необходимости — к примеру, пополнить баланс своего сотового телефона.

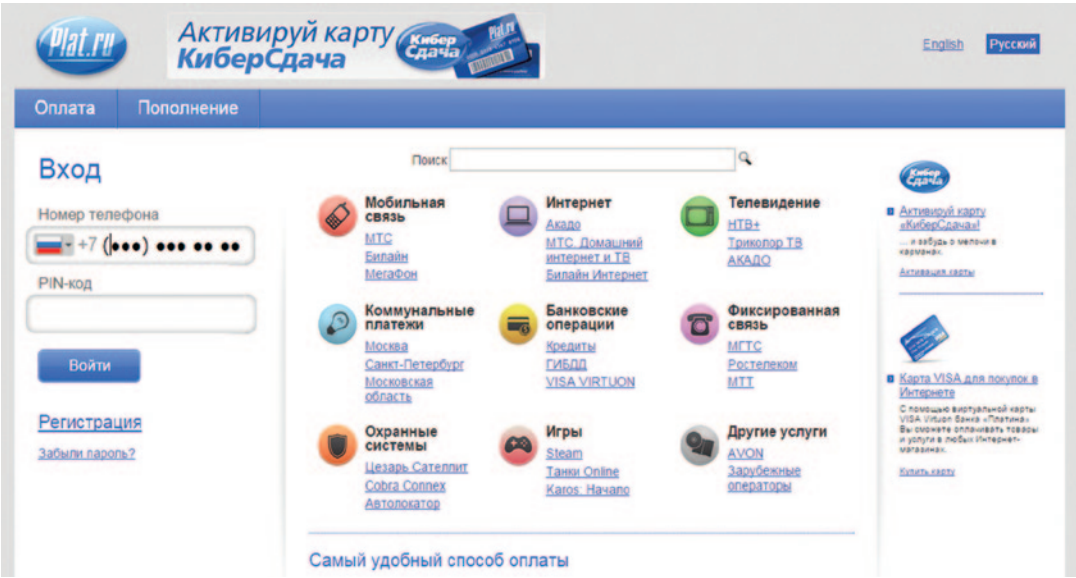
Создать Платёжную книжку

Ваш номер телефона: 8 (916) 123-45-67

Введите текст на картинке: tuburg

☒ Я согласен с условиями [Публичной Оферты](#)

Создать



Интерфейс «Платёжной книжки»

Сервис Plat.ru — «Платёжная книжка КиберПлат» позволяет:

- производить платежи с баланса на веб-сайте в адрес провайдеров услуг;
- сохранять реквизиты частых платежей;
- регистрировать новых провайдеров услуг для проведения платежей;
- отслеживать историю платежей.

Возможности для партнёров

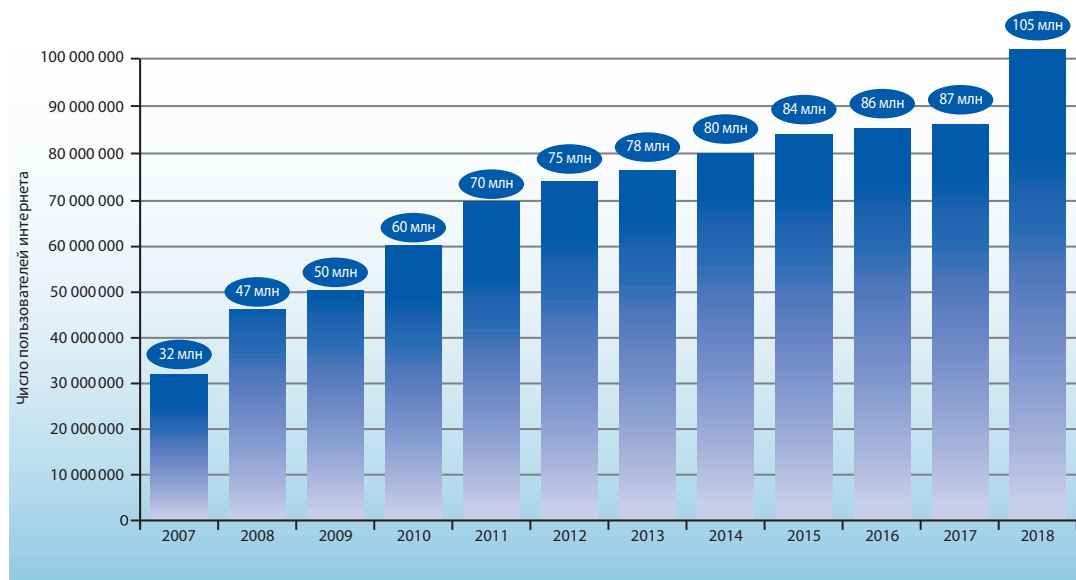
Бизнес-схема проекта предусматривает распределение комиссии провайдеров услуг, в пользу которых будут проводиться платежи, между компанией «КиберПлат» (CyberPlat®) и теми агентами, которые провели первичную регистрацию пользователей.

Для партнёров системы электронных платежей «КиберПлат» (CyberPlat®), таким образом, обеспечена возможность получения дополнительных доходов как за счёт комиссии с клиентов при пополнении баланса «Платёжной книжки», так и за счёт участия в доходах от комиссии провайдеров услуг, в чью пользу проводятся платежи с баланса нового сервиса.

Возможности для банков

Plat.ru — «Платёжная книжка КиберПлат» может быть использована в качестве сверхоблегченной версии Интернет-Банк-Клиента. Почему это важно и может быть крайне выгодно для банков?

- В России сегодня 105 миллионов пользователей интернета и их становится всё больше.
- Оборот интернет-банкинга в России в 2018 году, по экспертным оценкам, достиг 2,4 триллионов рублей.
- Число активных пользователей интернет-банкинга в 2018 году в РФ оценивается в 37 миллионов человек.
- Рынок электронных продаж России за 2018 год оценивается в 1,66 триллионов рублей.



Почему это происходит?

Причины в следующем.

- Современные системы ИБ сложны в использовании. Они требуют повышенной квалификации пользователей.
- Системы ИБ перегружены избыточным функционалом.
- Практически нет «однокнопочных» решений — любой терминал проще в использовании.
- Именно поэтому «КиберПлат» (CyberPlat®) предлагает банкам «Платёжную книжку» — удобный, простой и доступный, не требующий особой квалификации пользователя инструмент для совершения платежей.

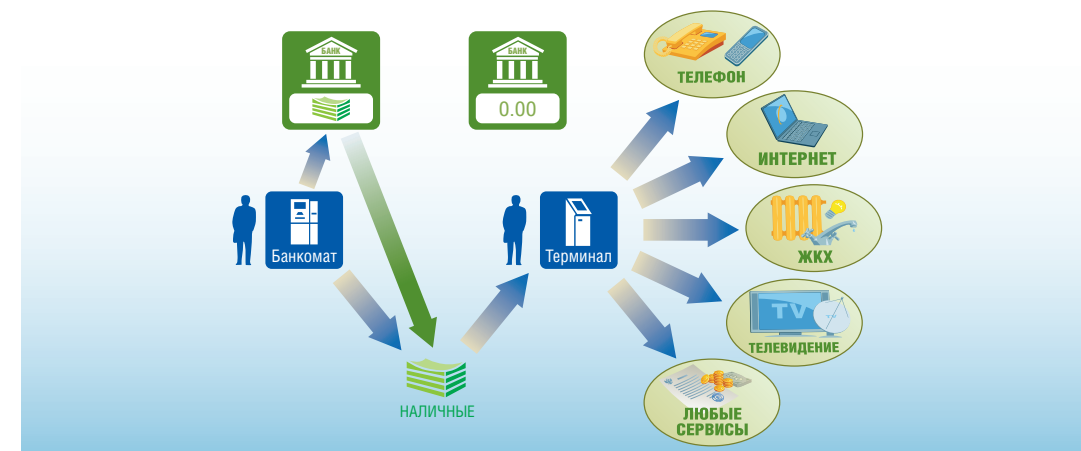
Ключевые преимущества «Платёжной книжки»

- Простой и интуитивно понятный интерфейс.
- Использование не только через сайт, но и на cash-in-терминалах.
- Простое и быстрое пополнение баланса наличными.
- Отсутствует необходимость полной идентификации при открытии персональной учётной записи, поскольку платежи ограничены суммой в 15 тысяч рублей, а таких платежей подавляющее большинство.
- Клиент боится хранить деньги в банках, поэтому вносит наличные в терминал, наличные тут же конвертируются в пополнение баланса «Платёжной книжки», и клиент сразу платит по ранее созданному шаблону.
- Остаток от «некруглых» платежей не пропадает, а сохраняется на балансе книжки.

Использование «Платёжной книжки» в качестве облегченной версии системы Интернет-Клиент-Банк дает банкам возможность резко увеличить число клиентов и охватить максимум из 105 миллионов пользователей интернета.

Большим преимуществом является и отсутствие сколько-нибудь значимых затрат на внедрение «Платёжной книжки».

В отличие от аналогичных продуктов и разработок, «Платёжная книжка» распространяется по принципу White Label/API, и банки-партнёры могут использовать этот универсальный и простой в эксплуатации продукт под своим брендом.

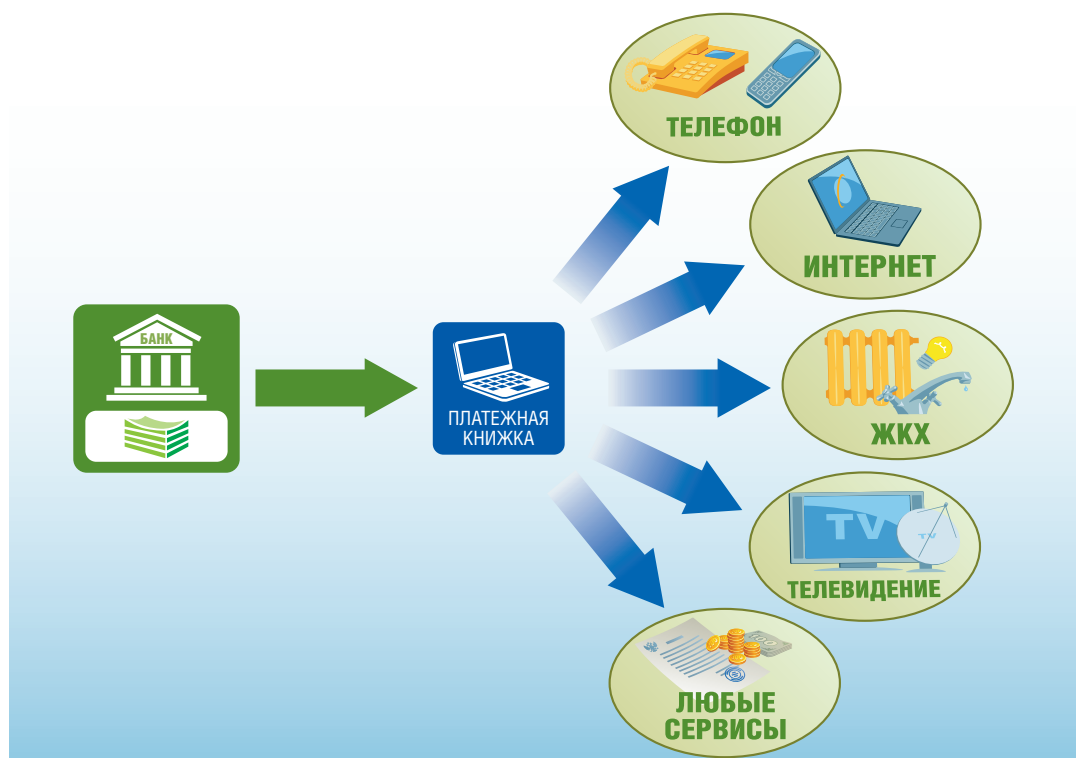




При использовании «Платёжной книжки» в качестве собственного продукта доходы от осуществления платежей распределяются между «КиберПлат» (CyberPlat®) и банком-партнёром.

Банк-партнёр получает следующие преимущества:

- Резкое увеличение количества клиентов.
- Захват сектора низкодоходных клиентов.
- Увеличение доли комиссионных доходов в структуре доходов.
- Экономия денежных средств на разработке и внедрении собственных систем Интернет-Банк-Клиент.
- Увеличение остатков на счетах.
- Продвижение бренда банка как «социально полезного».



Возможности для провайдеров услуг

На базе «Платёжной книжки», этого простого технологического решения, возможна реализация нового прибыльного сервиса «Платёжи с лицевого счёта» для клиентов операторов связи, поставщиков интернета и коммерческого ТВ, других провайдеров массовых услуг. Внедрение такого сервиса увеличивает лояльность абонентов и положительно сказывается на росте капитализации бизнеса.

В настоящее время наблюдается отчётливый тренд в сторону создания и развития подобных сервисов всеми ведущими операторами мобильной и фиксированной связи, операторами интернета и коммерческого телевидения. Выгоды от развития данного сервиса очевидны.

- Во-первых, клиентам предлагается удобный платёжный инструмент, за счёт чего:
 - расширяется спектр услуг;
 - повышается качество обслуживания.
- Во-вторых, компании получают дополнительную прибыль за счёт получения комиссионного дохода от регулярных платежей абонентов с их лицевых счетов.
- В-третьих, увеличиваются и «цементируются» остатки на лицевых счетах клиентов и снимаются проблемы, вызываемые периодически возникающей задолженностью и необходимостью отключать клиентов от пользования платными услугами.

Стало уже привычным, что пополнение счёта поставщика услуг (например, мобильного оператора или провайдера интернета) возможно практически в любой розничной точке или платёжном терминале. Но с сервисом «Платёжи с лицевого счёта» от «КиберПлат» (CyberPlat®) ситуация обратная. С помощью лицевого счёта в биллинговой системе оператора клиенты смогут оплачивать те же коммунальные услуги, доступ в интернет, пополнять банковские счета, осуществлять денежные переводы и многое другое. Реализация этого решения практически не требует расходов и сколько-нибудь значимых трудозатрат.

Опыт показывает, что внедрение предлагаемого сервиса возможно в течение двух недель. В то же время дополнительный доход начнёт генерироваться сразу же после запуска сервиса в эксплуатацию. Партнёрская программа White Label позволяет операторам запустить сервис «Платёжи с лицевого счёта» под своим брендом. Для этого потребуется лишь изменение внешнего вида экранных интерфейсов и их оформление в фирменном стиле оператора.



Специалистами «КиберПлат» (CyberPlat®) разработана и успешно эксплуатируется ещё один сервис платежей через интернет — TopUp.ru (www.topup.ru), который позволяет осуществлять платежи в адрес широкого круга провайдеров с помощью банковских карт.

Платёжи можно осуществлять с карточных счетов в Банке «Платина» — это может быть специальная неперсонифицированная банковская карта VISA Electron Банка «Платина», к которой привязана услуга проведения платежей в пользу провайдеров, либо персонифицированная платёжная карта Банка «Платина», зарегистрированная в проекте «Экономия».

Платёжи в сервисе TopUp.ru можно осуществлять и с карточных счетов других российских банков-эмитентов.

Использование карт, участвующих в проекте «Экономия» Банка «Платина», позволяет сэкономить на комиссии по карточным транзакциям и получить скидку при оплате услуг провайдеров. Карты распространяются в офисах Банка «Платина» (www.platina.ru), где можно как получить неперсонифицированную карту «Экономия», так и зарегистрировать в этом проекте уже имеющуюся карту Банка «Платина».

Если клиент уже имеет платёжную карту Банка «Платина», он может зарегистрировать её в проекте «Экономия». После регистрации можно воспользоваться тем же набором услуг, что и владельцы карт «Экономия».

После регистрации на выбор клиента предоставляется несколько вариантов выполнения платежей:

- с мобильного телефона с помощью программы CyberplatMobile;
- с домашнего компьютера через сервис <http://topup.ru>.

Сразу после заполнения анкеты и вручения карты «Экономия» специалисты «КиберПлат» (CyberPlat®) помогают клиенту установить на мобильный телефон Java-приложение CyberplatMobile, создать и зарегистрировать в системе электронных платежей ключи электронной цифровой подписи и подключить услугу проведения платежей.

ВИРТУАЛЬНАЯ ПРЕДОПЛАЧЕННАЯ КАРТА VISA VIRTUON

В сети приёма платежей «КиберПлат» (CyberPlat®) реализована возможность приобретения виртуальных карт VISA для расчётов в сети интернет.

Виртуальную карту VISA можно приобрести на кассах торговых предприятий или в платёжных терминалах, подключённых к системе «КиберПлат» (CyberPlat®). Для этого клиент сообщает кассиру или набирает на мониторе платёжного терминала свой номер мобильного телефона. Система электронных платежей «КиберПлат» (CyberPlat®) проверяет наличие такого номера в учётной системе оператора связи и даёт подтверждение на совершение операции выпуска виртуальной карты. Далее клиент вносит ту сумму (до 15 тысяч рублей), которая составит номинал

выпускаемой карты и в пределах которой затем можно совершать платежи в сети интернет. После этого на номер сотового телефона, указанный клиентом, приходит SMS-сообщение с реквизитами виртуальной карты VISA.

Остаток денежных средств, не израсходованных после истечения срока действия карты, автоматически перечисляется на имеющуюся или специально для этого открытую учётную запись клиента в сервисе «Платёжная книжка КиберПлат», доступном через сайт plat.ru. Эти средства могут быть в дальнейшем использованы для расчётов с широким кругом провайдеров услуг, включая операторов сотовой связи.

Данный продукт представляет большой интерес для партнёров системы электронных платежей «КиберПлат» (CyberPlat®) — популярность виртуальных карт для расчётов в сети интернет быстро растёт одновременно с расширением ассортимента товаров и услуг, предлагаемых в глобальной сети. Комиссия Банка «Платина» за выпуск карты VISA составляет 3,5% от её номинала (не менее 25 рублей). При этом комиссия распределяется между Банком «Платина», системой электронных платежей «КиберПлат» (CyberPlat®) и агентом, оформившим выпуск карты.

Виртуальная карта VISA крайне полезна той категории населения, которая имеет и активно использует обычные банковские карты, но вполне обоснованно считает платежи в сети интернет операциями с высокой степенью риска. Также эта карта позволяет осуществлять платёжные операции в сети интернет тем пользователям, которые не имеют обычных банковских карт. Это граждане, не имеющие банковского счёта, а также молодые люди в возрасте до 16 лет, которым законодательно ограничена возможность получения обычных банковских карт. В то же время именно молодые люди составляют значительную часть интернет-аудитории и испытывают потребность пусть в небольших, но регулярных платежах в сети интернет.

Владельцы виртуальной карты VISA с её помощью могут оплачивать услуги популярных всемирных сетевых сервисов Skype, iTunes, Google, делать покупки через системы eBay, PayPal и в многочисленных интернет-магазинах, таких как amazon.com, а также оплачивать онлайн-игры. С помощью виртуальной карты VISA можно оплачивать авиабилеты на сайтах авиакомпаний и туристических агентств, а также приобретать железнодорожные билеты на сайте РЖД и многое другое.



ПОПОЛНЕНИЕ КАРТ VISA, MASTERCARD, МИР В СЕТИ «КИБЕРПЛАТ» (CYBERPLAT®)

Система электронных платежей «КиберПлат» (CyberPlat®) при участии международных платёжных систем Visa, MasterCard и российской НСПК «МИР» предоставляет услугу пополнения любых карт, выпущенных на территории РФ.

Технологически этот процесс осуществляется через специальные шлюзы, что позволяет передавать данные об операции пополнения конкретной карты в банк-эмитент практически мгновенно. Длительность зачисления средств непосредственно на счёт карты зависит от банка — эмитента карты и может либо быть моментальной, либо составлять от двух до четырёх дней.

Пополнение карт возможно в сетях платёжных терминалов и банкоматов, работающих через систему «КиберПлат» (CyberPlat®), в которых представлен этот сервис. Для пополнения любой карты достаточно ввести через интерфейс платёжного терминала или банкомата номер карты, а также внести необходимую сумму денежных средств.

Эта услуга, предоставляемая «КиберПлат» (CyberPlat®), широко востребована в целях регулярных выплат по полученным кредитам. Получатели кредитов, обладатели карт VISA, MasterCard и МИР, избавлены от необходимости посещения банковских отделений и могут производить операцию пополнения баланса карты в пунктах приёма платежей «КиберПлат» (CyberPlat®), расположенных в шаговой доступности — в магазинах, аптеках, на автозаправках и т.п.

Возможность удобного пополнения карт через сеть приёма платежей «КиберПлат» (CyberPlat®) повышает привлекательность пластиковых карт среди населения и делает их использование практичным.

MasterCard®
MoneySend™



МИР

VISA

КАК СТАТЬ ПАРТНЁРОМ «КИБЕРПЛАТ» (CYBERPLAT®)

СТАНЬ АГЕНТОМ СИСТЕМЫ «КИБЕРПЛАТ» (CYBERPLAT®) ЗА 5 МИНУТ! АВТОМАТИЧЕСКАЯ РЕГИСТРАЦИЯ АГЕНТОВ

В упрощённой процедуре сверхбыстрой автоматической регистрации используются возможности, предоставляемые ст. 428 Гражданского кодекса РФ, согласно которой агент присоединяется к Договору о приёме платежей (Договор присоединения, с которым можно ознакомиться на сайте <http://www.cyberplat.ru/agent/dogovor.pdf>), просто подав соответствующее Заявление.

Значительно упрощена процедура формирования ЭП и работы с агентской сетью за счёт объединения всех необходимых действий в рамках одного программного модуля «Менеджер ключей». После регистрации пользователь скачивает эту программу и, следуя указаниям «мастера», создаёт комплект ключей и регистрирует свой открытый ключ в системе. Администратор может самостоятельно в «Кабинете агента» зарегистрировать торговую точку или кассира, получить карточки ключей для них, сформировать комплект ключей с помощью «Менеджера ключей» и зарегистрировать открытые ключи в «Кабинете агента». Упрощённая процедура регистрации в системе электронных платежей «КиберПлат» (CyberPlat®) позволяет быстро подключиться к системе без открытия расчётного счёта и без личного присутствия в офисе «КиберПлат» (CyberPlat®).

Для проведения автоматической регистрации необходимо выполнить следующие шаги.

1. Зайти на сайт в раздел «Регистрация нового дилера», заполнить регистрационную анкету и зарегистрировать Login и Password.
2. После первичной регистрации получить доступ в раздел «Кабинет агента». Используя Login и Password, необходимо отредактировать данные своей компании, зарегистрировать администратора, сформировать комплект ключей электронной цифровой подписи и получить пакет необходимых документов (заявление и акт приёма-передачи электронных ключей) в формате PDF.
3. После подписания заявления и акта в составе полного пакета документов их необходимо отправить заказным письмом в офис «КиберПлат» (CyberPlat®).
4. Специалисты компании проверят корректность документов, активируют нового агента и, подписав заявление и акт со своей стороны, направят экземпляр адресату.
5. Агент может самостоятельно регистрировать в системе свои пункты приёма платежей и кассиров через «Кабинет агента» и начинать приём платежей либо через веб-интерфейс, либо с помощью программы «Приём платежей», которую необходимо скачать с сайта www.cyberplat.ru и настроить.



Все процедуры автоматической регистрации выполняются с помощью максимально оптимизированного эргономичного интерфейса и в совокупности занимают не более пяти минут. При возникновении малейших проблем на любом этапе регистрации можно проконсультироваться по телефону у специалистов службы поддержки «КиберПлат» (CyberPlat®), указанному на сайте http://www.cyberplat.ru/join/dealer/about_reg/.

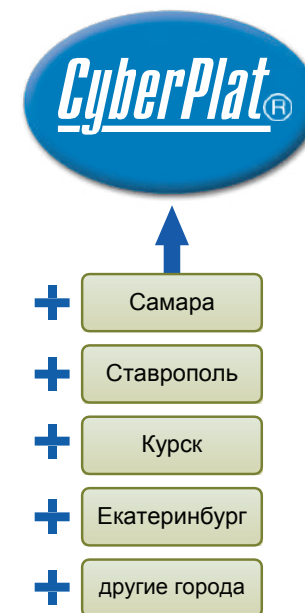
СТАНЬ РЕГИОНАЛЬНЫМ ПРЕДСТАВИТЕЛЕМ СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ «КИБЕРПЛАТ» (CYBERPLAT®)!

В рамках уникальной программы «Региональный представитель «КиберПлат» (CyberPlat®)» партнёром системы можно стать даже без организации своих точек приёма платежей. Цель данной программы — предоставить активной части российских предпринимателей возможность увеличить собственные доходы, дать упрощённый инструмент по привлечению новых торгово-сервисных предприятий в сеть приёма платежей «КиберПлат» (CyberPlat®).

Не обязательно иметь юридические (договорные) отношения с компаниями, которые региональный представитель привлекает в систему электронных платежей «КиберПлат» (CyberPlat®), не обязательно быть и агентом системы электронных платежей.

Региональному представителю нет необходимости:

1. Заключать договор с агентом (торгово-сервисные точки которого могут принимать платежи).
2. Держать остаток средств в системе электронных платежей «КиберПлат» (CyberPlat®) в размерах, необходимых для деятельности агента системы электронных платежей.
3. Организовывать собственные точки приёма платежей (аренда помещений, регистрация кассовых аппаратов, штат сотрудников).
4. Организовывать субагентскую сеть приёма платежей (договоры с третьими компаниями, организация инкассации, денежные переводы).
5. Нести ответственность своими денежными средствами перед системой электронных платежей «КиберПлат» (CyberPlat®) за платежи, принятые и проведенные другими компаниями.
6. Принимать платежи от абонентов операторов связи и клиентов провайдеров услуг.



Региональному представителю для начала работы необходимо:

- 1. Получить статус индивидуального предпринимателя или юридического лица.
- 2. Заключить Агентский договор с системой электронных платежей «КиберПлат» (CyberPlat®).

Обязанности регионального представителя:

- 1. Поиск торгово-сервисных точек (юридических лиц или индивидуальных предпринимателей), желающих организовать приём платежей. Региональный представитель самостоятельно определяет стратегию привлечения агентов.
- 2. Разъяснение потенциальному агенту всех преимуществ системы электронных платежей «КиберПлат» (CyberPlat®), удобства подключения к ней через интернет.
- 3. Помощь в проведении регистрации.
- 4. Консультации по вопросам оптимизации процесса проведения платежей и правильности работы с системой электронных платежей «КиберПлат» (CyberPlat®).
- 5. Ежедневное предоставление отчёта о подключённых агентах.
- 6. Ежемесячное подписание акта о выполненных работах (список агентов, подключённых за отчетный месяц).

На указанный перечень работ региональный представитель получает доверенность от ООО «КИБЕРПЛАТ».

Вознаграждение.

Вознаграждение выплачивается ООО «КИБЕРПЛАТ» на основании заключенного с региональным представителем договора. Размер вознаграждения регионального представителя составляет 0,1% от месячного объёма платежей привлечённого агента. Например, региональный представитель за месяц привлёк трёх агентов.

Агент	Оборот агента за месяц (USD)	Вознаграждение (0,1%) за месяц (USD)
Первый	300 000	300
Второй	1 000 000	1000
Третий	1 500 000	1500
Всего	2 800 000	2800

Ограничения заработка нет!

Все зависит от возможностей и способностей регионального представителя. Регистрация региональных представителей системы электронных платежей «КиберПлат» (CyberPlat®) проводится на сайте компании: <http://www.cyberplat.ru/join/representative/reg> или по телефону +7(495) 967-02-20.

СYBERFT — УДОБНАЯ
И БЕЗОПАСНАЯ СИСТЕМА
ОБМЕНА ФИНАНСОВЫМИ
СООБЩЕНИЯМИ

ПЛАТФОРМА CYBERFT

Платформа CyberFT — высокотехнологичная российская разработка, представляющая собой ИТ-платформу с поддержкой самых современных форматов обмена данными, включая SWIFT InterAct, SWIFT FileAct и SWIFT Fin (все документы категории MT), а также комплект документов в форматах Банка России, необходимый для оказания услуг дистанционного банковского обслуживания, с возможностью создавать новые банковские сервисы.



SWIFT: СУЩЕСТВУЮЩИЕ ОГРАНИЧЕНИЯ

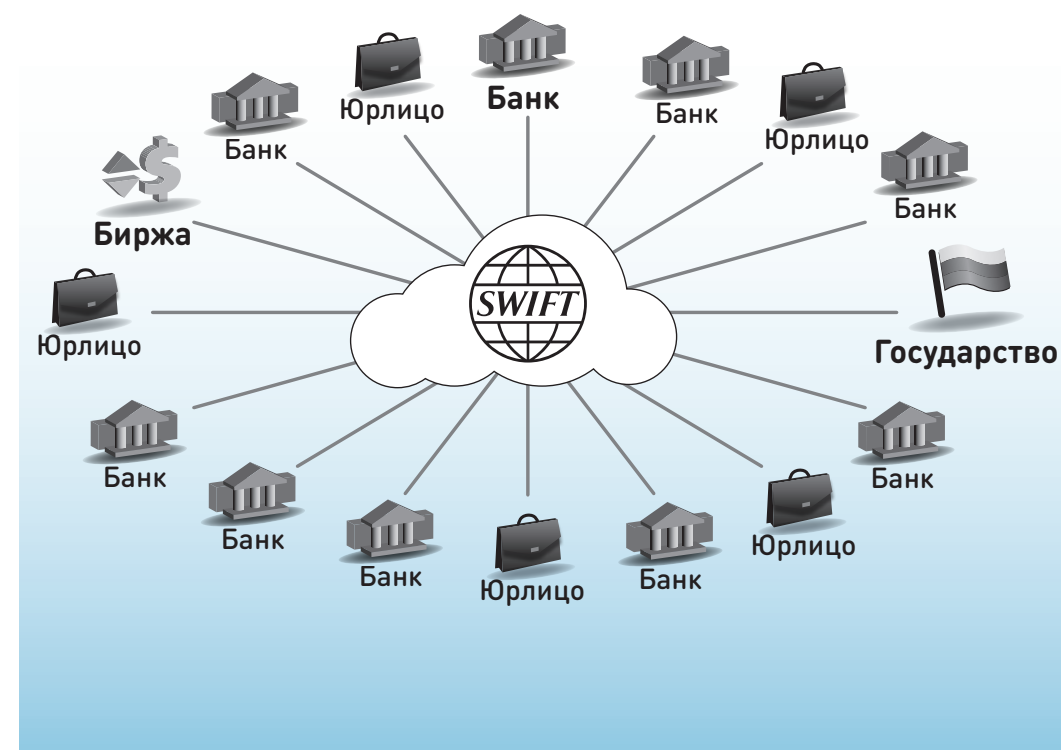
До выступления Эдварда Сноудена о массовой слежке банковское сообщество почти не задумывалось над рисками и лимитирующими факторами, которые существуют при использовании международной системы обмена банковскими сообщениями SWIFT.

- Монополия системы SWIFT, которая занимает около 90% рынка.
- Высокая политическая зависимость (примеры: отключение Ирана в 2012 году, периодические угрозы в адрес России, особенно в период введения санкций).
- Устаревшая топология сети SWIFT, так называемая звезда, надёжность которой в случае целенаправленной атаки подвергается угрозе.
- Всего 4 центра обработки данных, расположенных в трёх странах (США, Нидерланды и Швейцария).
- Законодательные ограничения: в соответствии с Федеральным законом РФ 161-ФЗ «О национальной платёжной системе» информация по внутренним платежам не должна выходить за пределы страны.

- Невозможность смены метода шифрования на выбор участника системы.
- Доступность передаваемых данных оператору сети, что порождает риски масштабной утечки коммерческой информации.
- Сложность признания передаваемых сообщений юридически значимыми.
- Ограниченный срок хранения данных на стороне SWIFT до их переноса в архив — до 121 дня.
- Негибкость форматов сообщений и сложность их адаптации к специфике форматов определённой страны.
- Высокая стоимость подключения и обслуживания.

Специалисты по безопасности многие годы обращали внимание на уязвимость такой схемы и на то, что во всех развитых странах локальной (внутристрановой) банковской информации законодательно запрещено покидать территорию своей страны. Например, в странах Евросоюза персональная информация (финансовые транзакции часто содержат персональные данные) не может обрабатываться в стране, расположенной за пределами Евросоюза, если последняя не обеспечивает должного уровня защиты персональных данных. Народный банк Китая (НБК) в начале 2011 года выпустил «Уведомление для банковских финансовых институтов» с требованием о защите финансовой информации. Документ, среди прочего, запрещает банкам хранение, обработку или анализ за пределами страны любой персональной финансовой информации, которая была собрана в Китае.

Таким образом, внутригосударственные межбанковские сети связи должны быть автономны, иначе суверенитет страны оказывается под угрозой и может зависеть от недружественных действий со стороны США или иных сил.

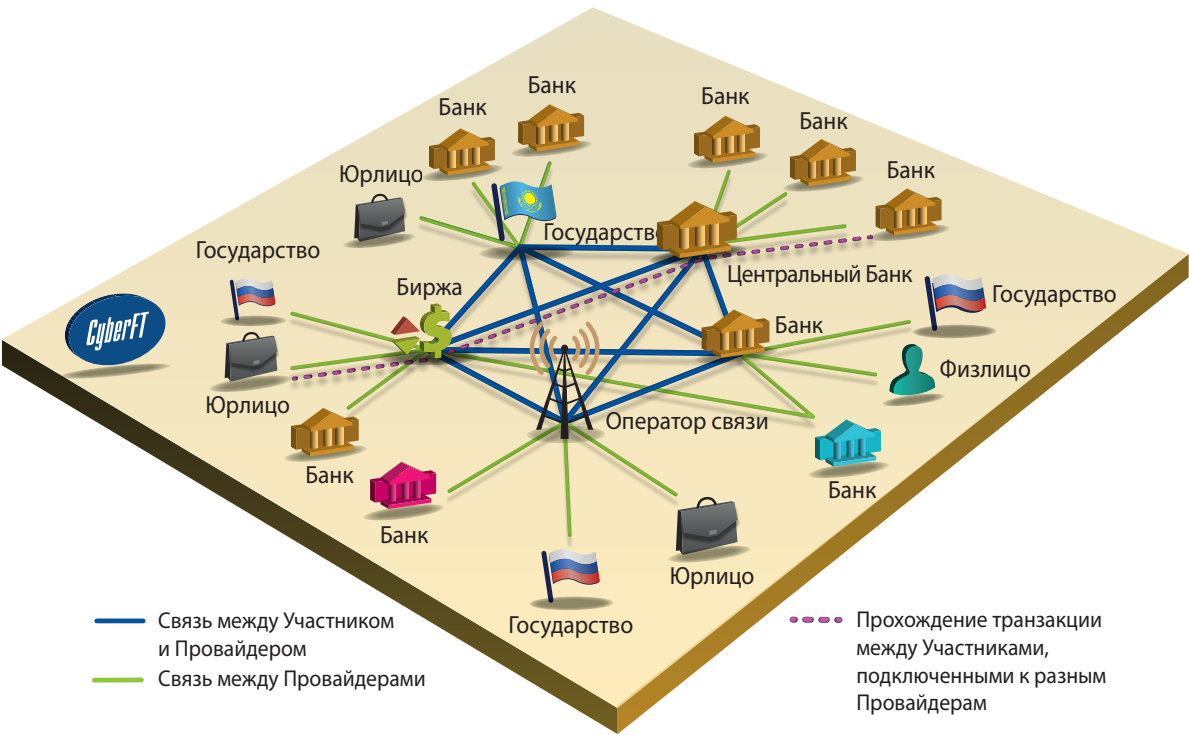


НОВЫЙ ПОДХОД К ОБМЕНУ ФИНАНСОВЫМИ СООБЩЕНИЯМИ

CyberFT — это универсальная система защищённого электронного обмена финансовыми данными и юридически значимыми документами между кредитно-финансовыми организациями, органами государственной власти, юридическими и физическими лицами (www.cyberft.ru).

В отличие от множества других систем, работающих на мировом рынке, это программное обеспечение разработано российскими специалистами и обладает лицензионной и патентной независимостью.

Условия сотрудничества предполагают, что все серверы платформы CyberFT будут располагаться на локальной территории страны — покупателя платформы, поэтому вероятность утечки коммерчески важных данных в электронном документообороте резко уменьшается.



ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Программно-аппаратное решение, реализующее информационную защищенную магистраль передачи любых типов электронных сообщений. Платформа CyberFT	Юридическое лицо, привилегированный участник CyberFT, управляющий Процессингом. Провайдер CyberFT	Программно-аппаратное решение, реализующее юридически значимый электронный документооборот в Сети CyberFT. Процессинг CyberFT
Юридическое или физическое лицо, использующее связь с Провайдером CyberFT для обмена информацией. Клиент CyberFT	Программное обеспечение, установленное на стороне Клиента CyberFT для взаимодействия с Сетью CyberFT. Клиентское ПО	Совокупность Провайдеров и Клиентов, подключившихся к CyberFT. Сеть CyberFT

CYBERFT, SWIFT И СПФС

Первый релиз системы CyberFT был выпущен в 2014 году и сразу объединил в себе практически полный функционал SWIFT Fin с целым рядом дополнительных опций, разработанных с применением самых современных технологий, недоступных в SWIFT. Ближе к концу 2014 года Банк России в ответ на санкции и угрозы Запада по отключению России от SWIFT разработал сервис по передаче финансовых сообщений СПФС, который представил банковскому сообществу в качестве полноценной замены SWIFT на территории РФ.

Таким образом, CyberFT одновременно конкурирует с двумя системами. С одной стороны, платформа успешно доказывает своё преимущество перед системой с многолетней историей и обширной клиентской базой, но крайне негибкой, устаревшей и сложной с точки зрения применяемых технологий, а также дорогостоящей и политически зависимой. С другой стороны, CyberFT соперничает с молодой и малофункциональной системой, обладающей сильным административным ресурсом.

	SWIFT	СПФС	CyberFT
Клиенты	Около 10 тысяч банков и ограниченное количество юридических лиц	Кредитные организации и их филиалы — клиенты Банка России (только имеющие SWIFT BIC)	Потенциальная возможность охвата всех банков и всех юридических лиц без ограничений
География услуг	Весь мир	Российская Федерация	Весь мир
Соответствие законодательству РФ	Не соответствует ч. 11 ст. 16 ФЗ № 112-ФЗ от 5 мая 2014 года «О внесении изменений в Федеральный закон «О Национальной платёжной системе»	Полностью соответствует всем нормативно-правовым актам РФ	Полностью соответствует законодательству РФ
Время работы	24×7	Не работает с 21:00 до 7:00 по московскому времени, а также в выходные и праздничные дни	24×7
Шифрование	Шифрование СКЗИ от SWIFT	СКЗИ, применяемые при передаче электронных сообщений в платёжной системе Банка России (СКАД «Сигнатура»)	Любые сменные СКЗИ, включая CryptoPro, OpenSSL, Message-PRO, Агава и др.
Защищённость сообщений	Передаваемые данные доступны оператору сети	Передаваемые данные доступны оператору сети	Передаваемые данные не доступны оператору сети

	SWIFT	СПФС	CyberFT
Месторасположение серверов	США, Швейцария и Нидерланды	Российская Федерация	Россия, а также дополнительно в любой точке мира на усмотрение владельца платформы
Надёжность	Специальный порядок приёма и передачи сообщения за счёт «горячего» резервирования каждого элемента сети. Всего 4 центра обработки данных	Передача сообщений через Центр обработки сообщений Банка России (ЦОС) с использованием Среды взаимодействия с клиентами Банка России (СВК). Все информационные системы Банка России резервируются. Однако с учётом того, что вместе с ED503 был разработан целый ряд технических сообщений для проверки работы сервиса, можно сделать вывод о низкой надёжности системы	Эффективные современные программно-технические и организационно-административные меры обеспечения надёжности системы. Количество провайдеров не ограничено
Топология сети	Звезда (существует единый центр, к которому подключены все участники)	Звезда (существует единый центр, к которому подключены все участники)	Полносвязная (в системе может существовать бесконечное число центров, к которым подключаются различные участники, при этом сами центры также соединены между собой)
Цена подключения	Не менее \$53 тысяч с учётом обязательной прокладки кабеля от конкретного оператора услуги связи; до \$200 тысяч для каждого нового клиента	Бесплатно	Бесплатно
Цена транзакции	Сервис FIN: локальная транзакция 0,02–0,05 евро, международная 0,03–0,18 евро	Плата за передачу финансового сообщения внутри страны в формате SWIFT составляет 1,50–2,50 рубля (0,026–0,043 евро)	Не более 50% цены аналогичной транзакции SWIFT

	SWIFT	СПФС	CyberFT
Цена обслуживания	Не менее 10 тысяч евро в год	Бесплатно	Бесплатно
Время подключения	Не менее 8 недель при коллективном подключении. Не менее 16 недель при собственном подключении	Не менее 4–6 недель, так как на стороне АБС необходима платная доработка для передачи данных в терминал	Подключение к процессингу CyberFT от 1 до 3 недель, включая интеграцию с АБС. При установке собственной платформы — не более 2 недель
Скорость прохождения информации	Несколько секунд	Несколько секунд	Не более 1,5 секунд
Поддерживаемые форматы	Конверт для сообщений формата SWIFT Fin (сообщения MTXXX). При этом проверка корректности вводимой информации по правилам SWIFT не проводится, то есть фактически в конверт может быть помещено любое сообщение	Конверт для сообщений формата SWIFT Fin (при этом проверка корректности вводимой информации по правилам SWIFT не проводится, то есть фактически в конверт может быть помещено любое сообщение)	Сервис SWIFT Fin (сообщения MTXXX), сервис InterAct (сообщения MX в стандарте ISO 20022, адаптированные для России), FileAct (неструктурированные сообщения с вложениями), а также документы ЭДО (акты, счета-фактуры, контракты), приём платежей и многое другое
Максимальный размер одного сообщения	Не более 10 МБ	Максимальный размер по умолчанию — 20 КБ. Максимально возможный размер по отдельному разрешению — 5 МБ	Базовая настройка максимального размера одного сообщения составляет 100 МБ. При необходимости данный лимит может быть увеличен до любых размеров
Хранение информации	На стороне клиента срок не ограничен, на стороне процессинга SWIFT данные хранятся 124 дня, далее попадают в архив. Частично данные можно получить из архива на платной основе, но не всегда	В оперативном архиве электронные сообщения хранятся 3 дня, в долгосрочном архиве — 5 лет	Бессрочное хранение данных обо всех этапах прохождения транзакции от отправителя до получателя

	SWIFT	СПФС	CyberFT
Тип взаимодействия	Только процессинг	Только процессинг	Процессинг и клиринг
Пользовательский интерфейс	Несколько вариантов пользовательских приложений SWIFT Alliance для полноценной работы	Режим передачи финансовых сообщений формата SWIFT через АРМ КБР (КБР-С) с использованием каталогов файловой системы или менеджер очередей ЮМ MQ, осуществляется приём сообщений в транспортных конвертах на серверах СВК Банка России. Для реальной коммерческой эксплуатации требует доработки визуальных интерфейсов для пользователя и оператора	Удобный веб-интерфейс для полноценной работы с системой
Дополнительные сервисы для юридических лиц	Льготные условия работы для корпоративных клиентов в сравнении с банками, ПО SWIFT Alliance Lite и др.	Отсутствуют	Льготные условия работы для корпоративных клиентов, специализированный модуль для 1С, сервис электронного документооборота юридически значимых документов
Скорость разработки и доработок	Очень медленно, индивидуальные доработки и интеграционные модули не предлагаются	Посредственно, индивидуальные доработки и интеграционные модули предлагаются только для крупных участников	Оперативно, предоставляются типовые интеграционные модули, индивидуальные доработки и интеграционные решения. Возможны индивидуальные разработки на типовой платформе CyberFT

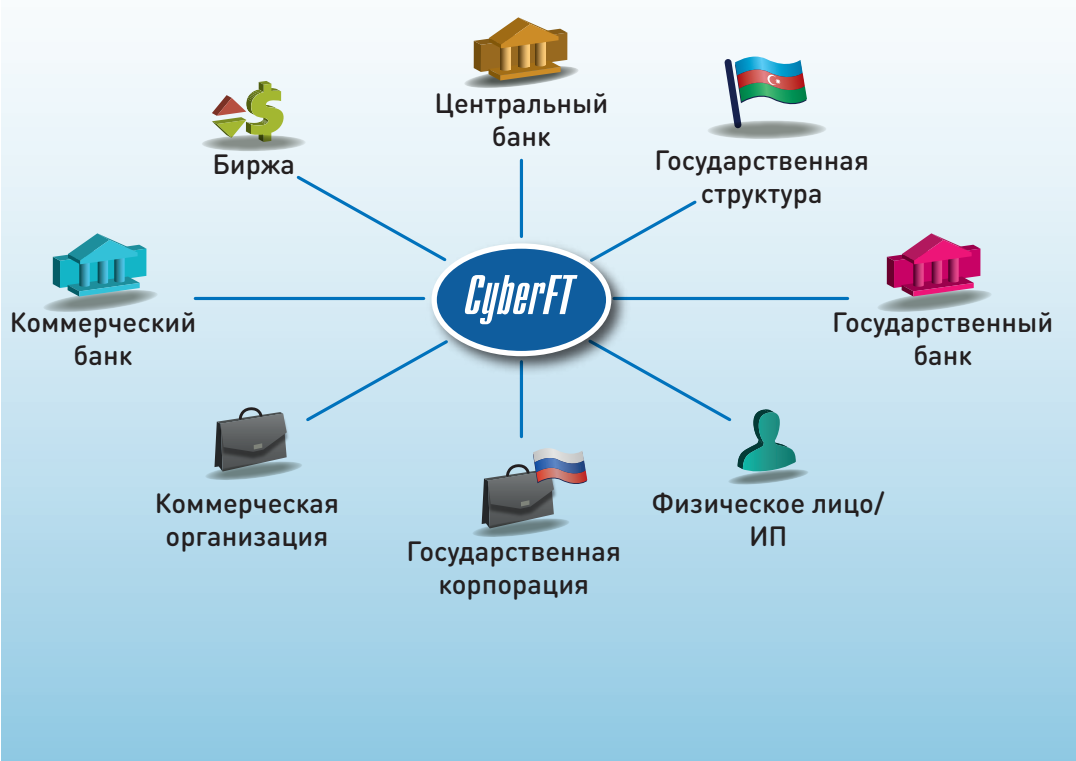
МНОГОПРОВАЙДЕРНОСТЬ

Сеть CyberFT состоит из неограниченного числа клиентов (участников), использующих для электронного документооборота платформу CyberFT.

Платформа CyberFT разворачивается на площадке покупателя и является независимой от компании «КиберПлат». Провайдер CyberFT может обслуживать банки и юридических лиц в любой точке мира или работать внутри отдельно выбранной банковской или корпоративной группы.

Провайдерами и участниками CyberFT могут выступать как банки, так и корпоративные клиенты, биржи, брокеры, органы государственной власти и другие организации. Каждому участнику присваивается уникальный идентификатор по правилам SWIFT (если участник не зарегистрирован в SWIFT) либо используется существующий идентификатор этого участника в сети SWIFT.

Справочник участников сети доступен каждому участнику и обновляется централизованно в автоматическом режиме. Идентификатор является уникальным не только в рамках одного провайдера, но и во всей сети CyberFT.



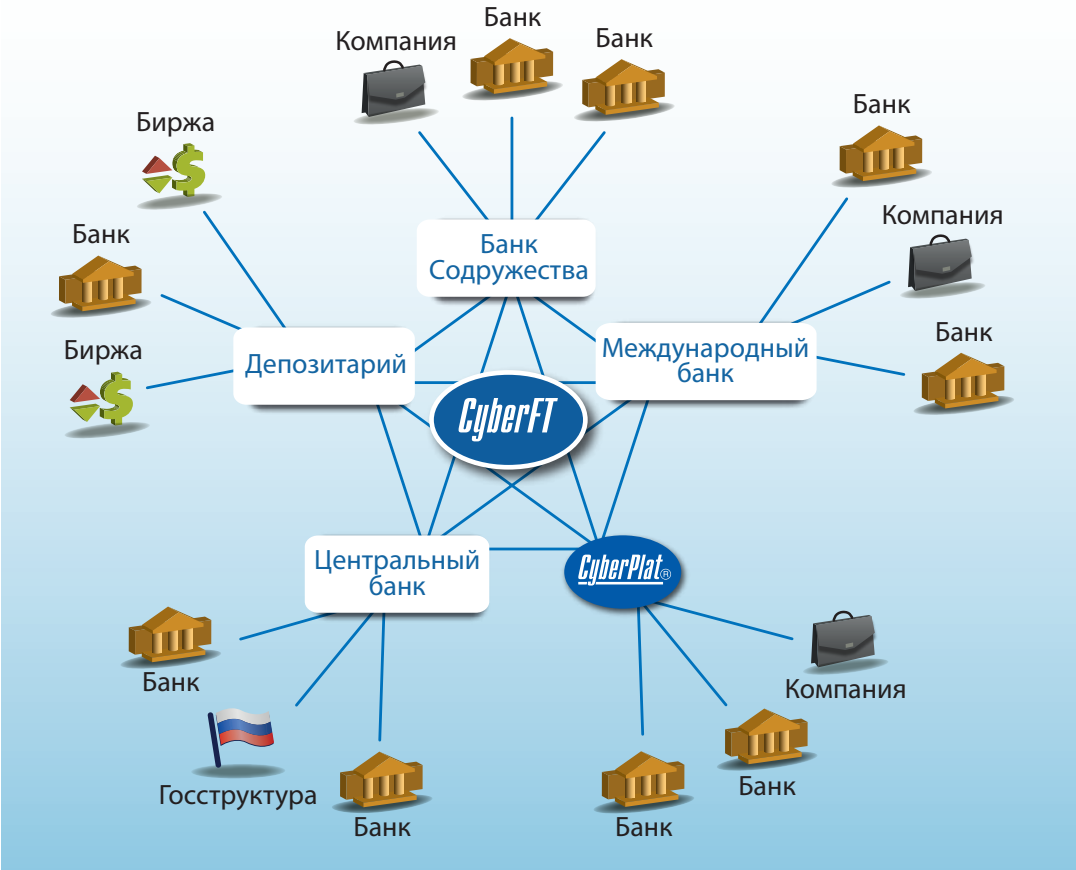
Таким образом, участник с определённым идентификатором может быть подключён только к одному провайдеру, что обеспечивает целостность сети.

Провайдеры CyberFT могут соединяться между собой различными способами, часть из которых представлена далее.

1. Каждый с каждым*

Информация о прохождении каждого сообщения логируется на стороне каждого провайдера, участвующего в его передаче. Более того, сами сообщения вместе с электронными подписями отправителя хранятся на стороне отправителя, получателя и провайдера в течение неограниченного срока (на стороне провайдера все сообщения хранятся в зашифрованном виде, и их содержимое недоступно провайдеру). Таким образом, каждый участник процесса обмена информацией имеет полноценные юридически значимые электронные документы.

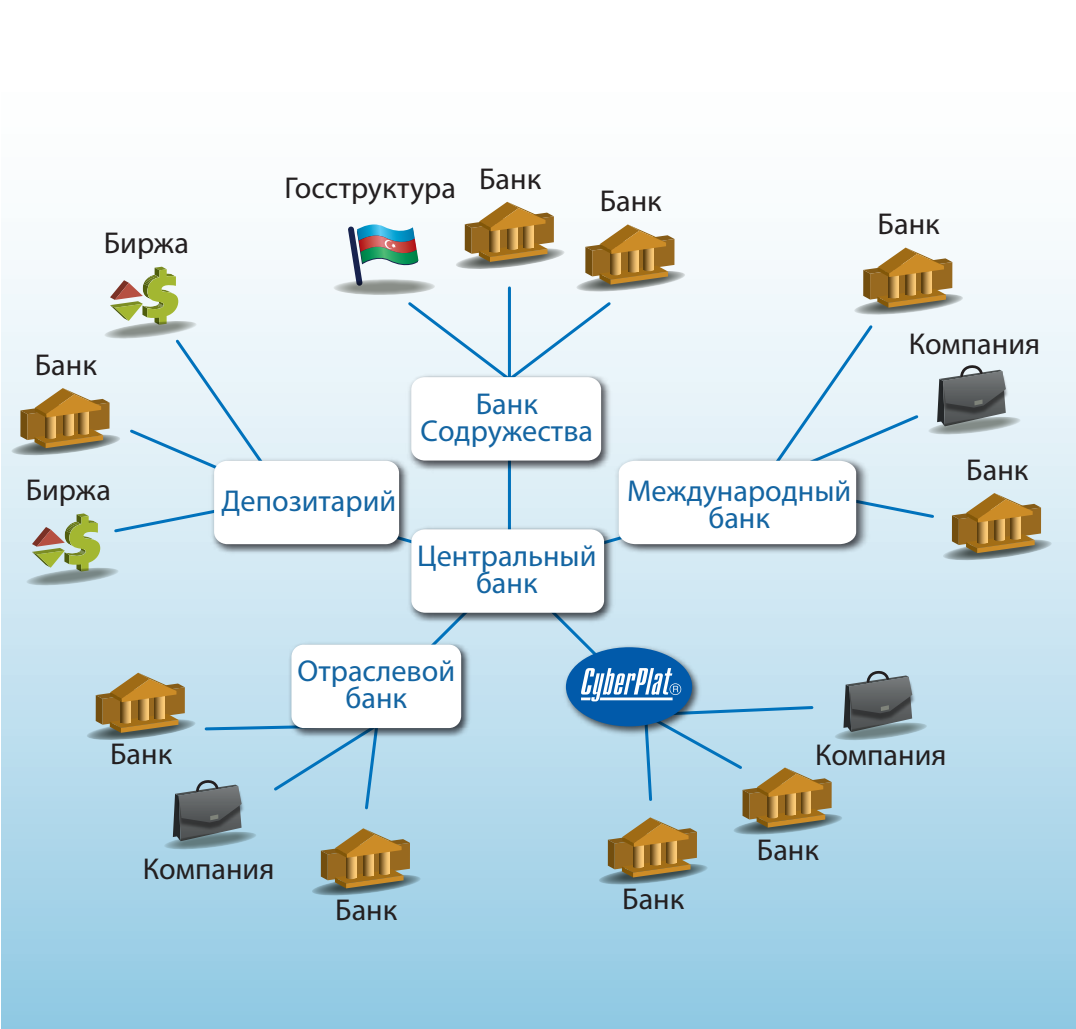
* Здесь и далее: названия организаций приведены в качестве примера



2. Через централизованного провайдера CyberFT, выбранного совместно

Например, любая крупная банковская группа или коммерческая организация может стать провайдером CyberFT и подключить дочерние организации, банки-корреспонденты и клиентов. При этом для обмена данными между участниками, подключёнными к разным провайдерам, эти провайдеры заключают соглашение с единым провайдером (например, Межгосударственным банком), который и отвечает за маршрутизацию сообщений между ними.

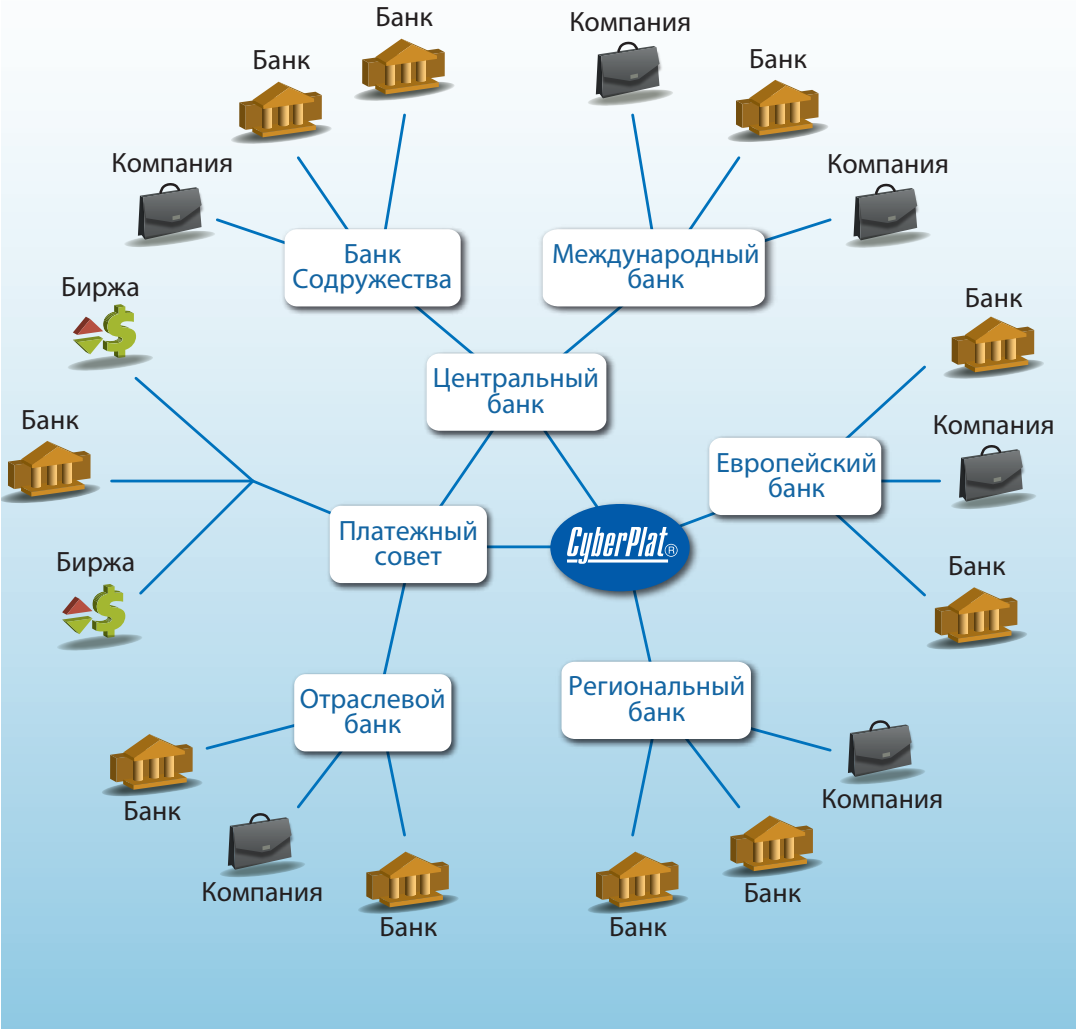
С одной стороны, такая топология сети существенно упрощает организационные моменты, связанные с установлением отношений между провайдерами, и позволяет работать через единую организацию (центрального провайдера), которой доверяют все участники. С другой стороны, в случае сбоя на стороне центрального провайдера связь между участниками сети будет невозможна.



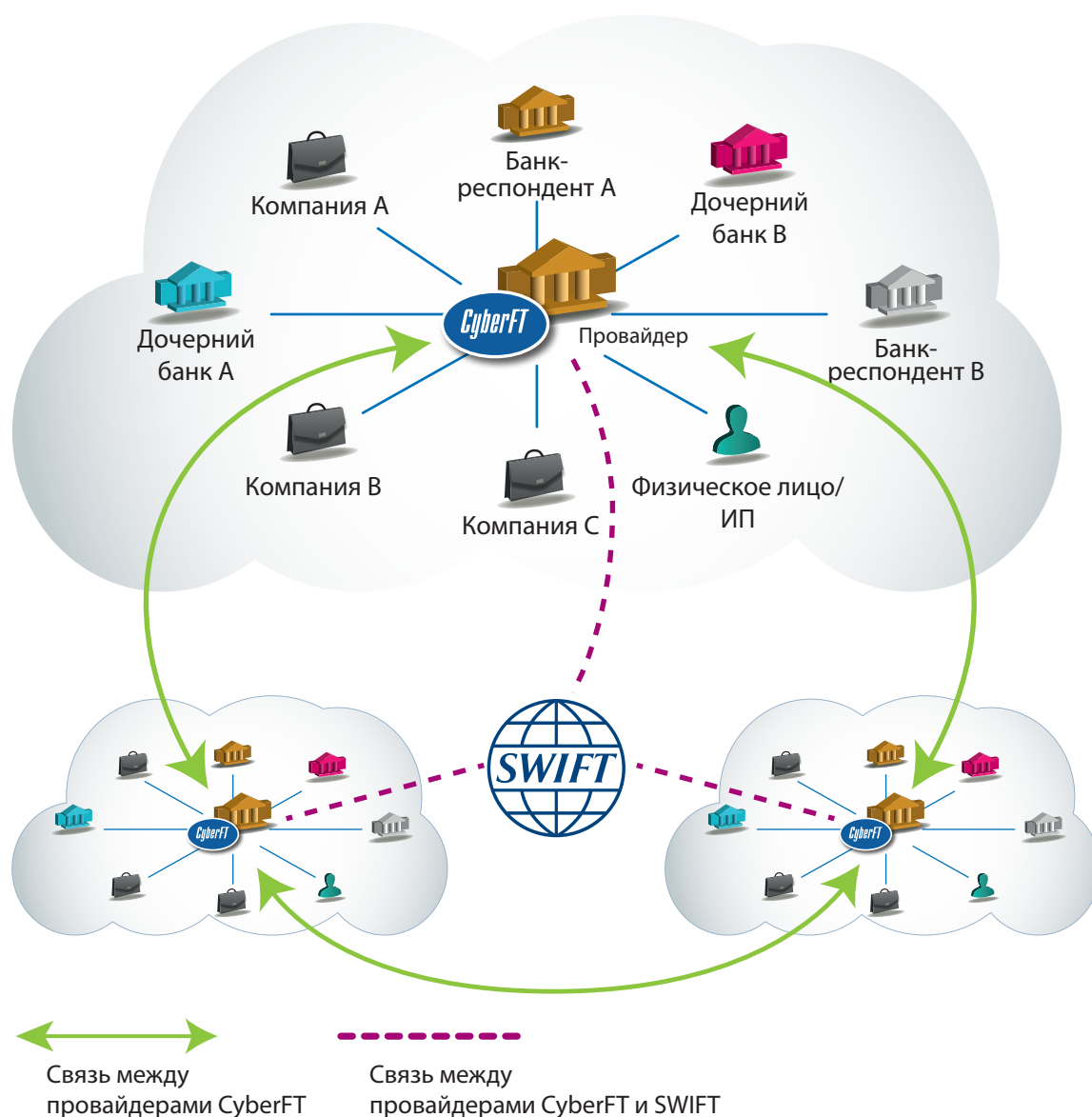
3. Через группу взаимосвязанных провайдеров CyberFT

Данный вариант топологии сети, несмотря на более сложные организационные процессы установления отношений между провайдерами, обладает повышенной отказоустойчивостью. В случае технических проблем на стороне одного из центральных провайдеров связь между всеми участниками сети CyberFT сохранится.

Участники сети CyberFT также могут взаимодействовать и с другими контрагентами, подключёнными к SWIFT. Один из примеров такого взаимодействия представлен на рисунке.



УНИВЕРСАЛЬНОСТЬ



Таким образом, сеть CyberFT позволяет участникам взаимодействовать и через систему SWIFT, если одна из сторон ещё не подключена к CyberFT (см. раздел, посвящённый вопросам интеграции и взаимодействия со SWIFT).

Сеть CyberFT необходима не только банкам, которые получают более безопасное, надёжное, функциональное, гибкое и экономически выгодное решение, но и клиентам кредитно-финансовых учреждений.

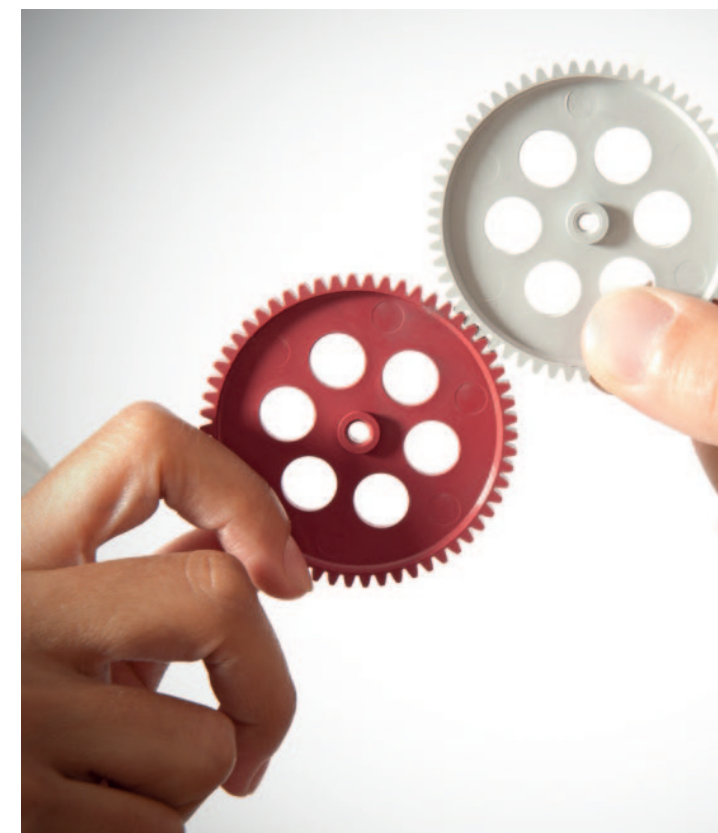
Компании крупного и среднего бизнеса, работающие одновременно с несколькими банками, в настоящий момент вынуждены поддерживать множество разных систем «Клиент-Банк», а также использовать различные форматы обмена данными и СКЗИ. CyberFT позволяет организовать для таких компаний «Универсальный Клиент-Банк».

На практике это означает, что достаточно составить финансовый документ (или сообщение) и выбрать нужный расчётный банк, после чего документ будет направлен по единому каналу в этот банк. Через этот же канал клиент будет централизованно получать обратную связь от своих расчётных банков (статусы по отправленным документам, выписки и т.д.). Таким образом, компании смогут взаимодействовать с банками напрямую через свою учётную систему, а также применять единые технологии при обмене данными.

Компания «КиберПлат» также разработала платёжный модуль для системы 1С, который позволяет клиентам дистанционно управлять счетами в своих расчётных банках прямо из 1С. При этом передача информации между 1С и банком осуществляется через сеть CyberFT.

В рамках универсального транспортного решения в сети CyberFT существует возможность реализации юридически значимого электронного документооборота. CyberFT позволяет оптимизировать бизнес-процессы, предусматривающие обмен документами с органами государственной власти: сдача налоговой отчётности, оформление таможенных деклараций, взаимодействие с государственной системой СМЭВ и др., а также межкорпоративные коммуникации, в том числе подписание контрактов, предоставление отчётной документации, подача биржевых заявок и т.д.

На базе CyberFT можно также построить такое необходимое для корпоративных клиентов решение, как межбанковский физический Cash Pooling.



БЕЗОПАСНОСТЬ

CyberFT является гарантом сохранности важной коммерческой информации. Одна из ключевых задач сети CyberFT — обеспечение безопасности информации, содержащей банковскую и коммерческую тайну. Согласно прогнозу компании Zecurion, по итогам 2018 года суммарные потери компаний и банков от утечек конфиденциальной информации могут превысить \$50 миллиардов.

Важная коммерческая информация, обрабатываемая платёжными системами и проходящая по каналам коммуникаций, подвергается целому ряду угроз.

1. Угроза безопасности межбанковских коммуникаций, поскольку в настоящий момент подавляющее большинство транзакций SWIFT проходит через серверы, находящиеся на территории США, Нидерландов и Швейцарии.

Размещение серверов в этих государствах ставит клиентов SWIFT в других странах в крайне уязвимое положение, так как в любой момент (например, при изменении политической обстановки) серверы могут быть отключены, что остановит не только обмен данными с иностранными банками-контрагентами, но и внутристрановой обмен финансовой информацией по системе SWIFT.

2. Угроза похищения непосредственно из системы, осуществляющей обработку и проведение платежа.

Информация может быть как «снята» по запросу спецслужб иностранного государства, так и перехвачена мошенниками или другими злоумышленниками на любом участке линий связи, длина которых может составлять вплоть до 20 тысяч километров. Использовать данную информацию, обычно относящуюся к банковской тайне, могут как сами похитители, так и лица, перехватившие её у похитителей (как это неоднократно происходило в громких международных скандалах последнего времени).

3. Угроза «слива» ранее украденной информации.

Громкие скандалы последних лет (например, дело Сноудена или появление WikiLeaks) говорят о том, что коммерческая информация, доступная спецслужбам, зачастую попадает в свободный доступ.



4. Угроза передачи информации конкурентам.

Примером такой утечки является скандал, разразившийся в 90-е годы в США, когда в результате перехвата переговоров Агентством национальной безопасности компания Airbus потеряла контракт объёмом \$6 миллиардов с национальной авиакомпанией Саудовской Аравии. Контракт достался компании McDonnell Douglas, являющейся подразделением Boeing — главного конкурента Airbus.

5. Угроза продажи украденной информации.

Информация является ценным товаром и чем более она значима, тем больше она стоит. Поэтому информация, содержащая коммерческую и банковскую тайну, является «лакомым куском» для международной киберпреступности. Защита от этих угроз регламентируется законодательством ряда стран, которые запрещают передачу локальной финансовой информации на территорию иностранного государства или предоставление доступа к ней с территории иностранного государства.

Использование платформы CyberFT значительно снижает все риски похищения, утери и продажи важной информации банков и их клиентов. Так как аппаратные средства будут находиться в вычислительном центре покупателя платформы, резко уменьшается угроза хищения коммерческой информации с серверов узла связи, а поскольку каналы коммуникации становятся намного короче, то существенно уменьшается риск хищения коммерческой информации с линий связи.

Текст сообщения, отправленный клиентом через сеть CyberFT и не адресованный провайдеру CyberFT, доступен только получателю сообщения другому клиенту CyberFT.

ПОДДЕРЖИВАЕМЫЕ ФОРМАТЫ, ГИБКОСТЬ И ВАРИАТИВНОСТЬ РАЗВИТИЯ

В настоящий момент в сети CyberFT полностью реализован сервис SWIFT Fin, включающий следующие группы сообщений:

- 1-я (клиентские платежи и чеки);
- 2-я (переводы финансовых организаций);
- 3-я (рынки финансовых ресурсов — форексные, денежные рынки и производные);
- 4-я (инкассо и кассовые письма);
- 5-я (рынки ценных бумаг);
- 6-я (операции с драгоценными металлами и синдицированными кредитами);
- 7-я (документарные аккредитивы и гарантии);
- 8-я (дорожные чеки);
- 9-я (управление денежными средствами и статус клиента);
- приём платежей «КиберПлат» (CyberPlat®).

Система поддерживает сервис SWIFT InterAct, то есть обмен сообщениями в форматах SWIFT MX (стандарт ISO 20022), и сервис SWIFT FileAct (обмен неструктурированными сообщениями, содержащими вложения объёмом до 100 МБ).

Система CyberFT содержит всё необходимое для обеспечения информационного взаимодействия между платёжными агентами и банками при осуществлении приёма платежей.

Система поддерживает необходимый для оказания услуг дистанционного банковского обслуживания (ДБО) комплект документов в форматах Банка России.

Одно из направлений развития системы — обеспечение защищённого комплексного информационного взаимодействия специализированных сфер бизнеса. В CyberFT можно обмениваться структурированными и неструктурированными договорами, актами, счетами-фактурами и другими типами документов. Благодаря интеграции с внутренними автоматизированными системами документооборота и делопроизводства организации могут реализовать сквозной электронный документооборот. Система CyberFT позволяет заключать и совершать сделки в электронном виде в соответствии с действующим законодательством.

Однако платформа CyberFT не ограничивается возможностями SWIFT. В ней для движения межбанковской информации можно предусмотреть столько «информационных полос» (категорий сообщений), сколько потребуется клиентам с учётом специфики их деятельности. Возможность подстроиться под нужды клиентов является краеугольным камнем построения любой надёжной и отлаженной системы, такой как CyberFT.

По запросу со стороны клиентов разработчики могут реализовать распространённую во всем мире систему Direct Debit. Причём данная система может быть создана либо в виде отдельной категории, либо в качестве дополнения к инвойсинговой категории SWIFT, либо в формате сервиса автоплатежей.

По запросу холдинговых компаний в рамках платформы CyberFT может быть разработано решение, позволяющее оптимизировать внутренний электронный документооборот, межбанковский Cash Pooling и другие востребованные рынком решения.

Компания «КиберПлат» в режиме онлайн анализирует предложения участников рынка и развивает функциональность CyberFT с учётом поступающей информации.

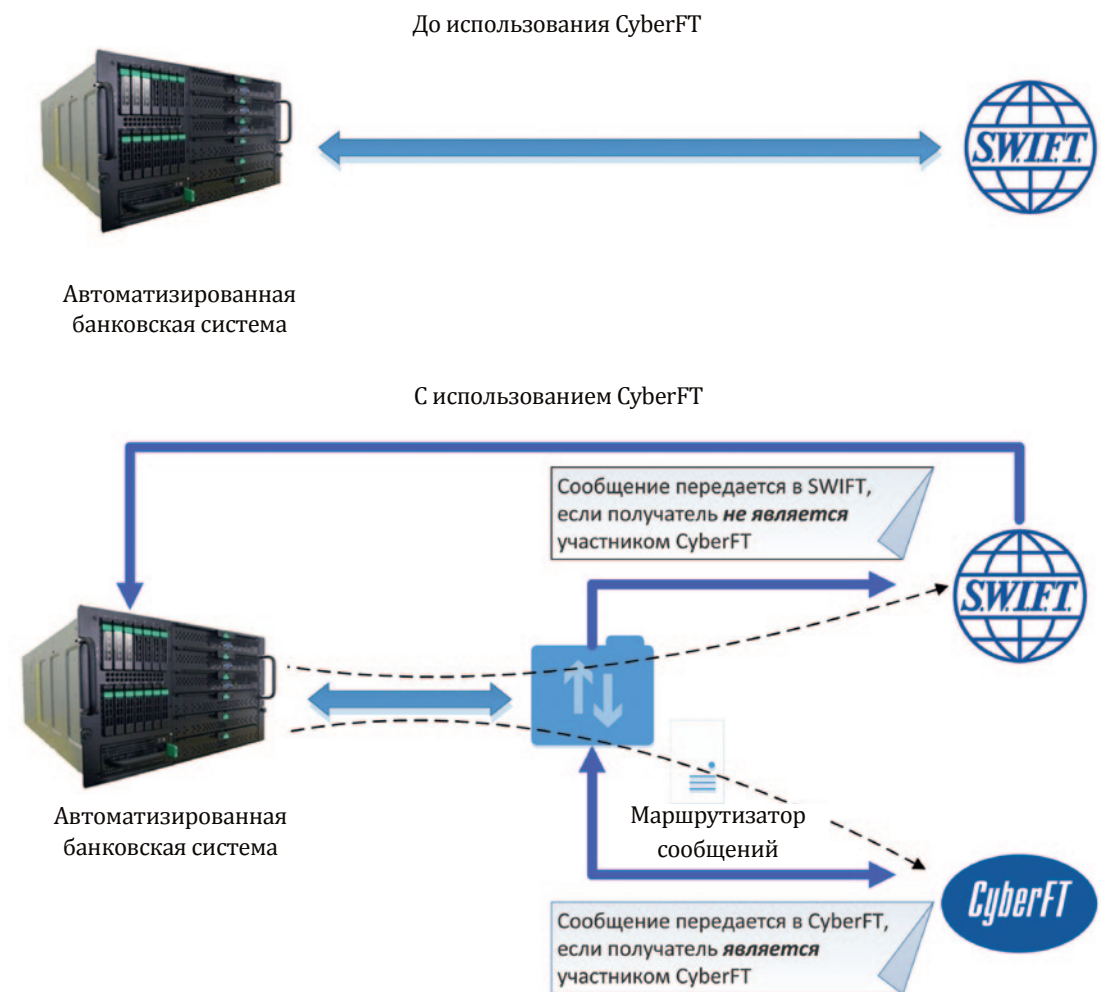
ВЗАИМОДЕЙСТВИЕ СО SWIFT. ПРОСТАЯ ИНТЕГРАЦИЯ ДЛЯ БАНКОВ

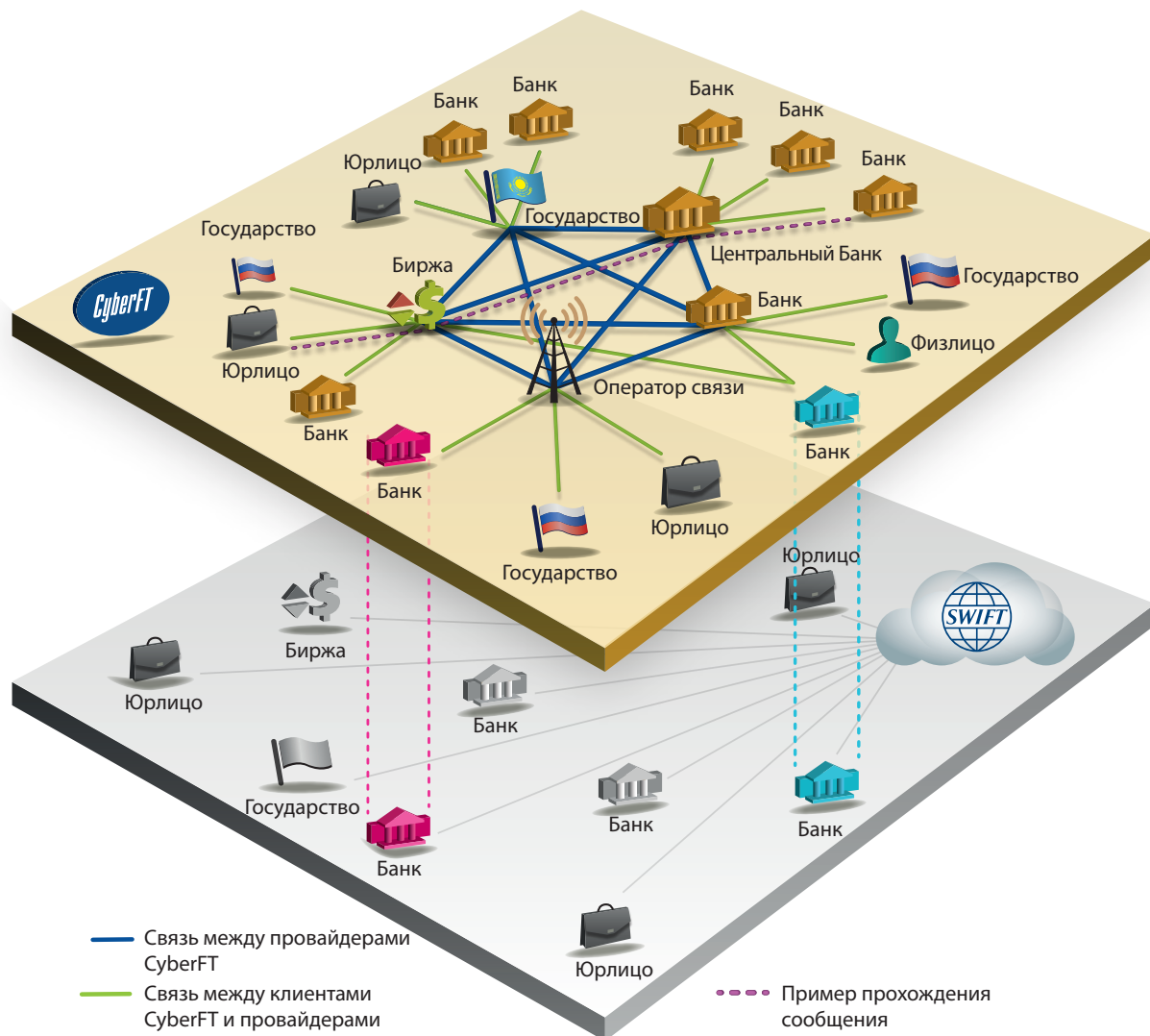
При подключении клиентов к платформе CyberFT клиентское программное обеспечение CyberFT может работать параллельно со SWIFT. Ниже приведена схема взаимодействия систем CyberFT и SWIFT на стороне клиента.

Специальный модуль «Маршрутизатор сообщений» в составе ПО CyberFT автоматически распределяет исходящие сообщения между CyberFT и SWIFT.

В случае если получатель сообщения не подключён к сети CyberFT, дальнейшее проведение транзакции осуществляется через систему SWIFT.

При этом клиент может задать гибкие параметры, которые позволят направлять исходящие сообщения строго в SWIFT, даже если получатель сообщения является участником CyberFT: например, определённым адресатам, определённого типа или категории, свыше пороговой суммы и т.д.





При подключении к CyberFT нового участника централизованный справочник участников будет обновлен дистанционно в автоматическом режиме. Программное обеспечение CyberFT предоставляется клиентам бесплатно.

CyberFT легко интегрируется со всевозможными учётными системами на стороне клиента и может работать вместе со SWIFT.

ДОСТУПНОСТЬ

Принципиальным отличием платформы CyberFT в сравнении со SWIFT является отказ от аппаратного шифрования и использование только программных методов шифрования. Подключение к сети CyberFT осуществляется через выделенный канал, VPN или публичный интернет, что предоставляет возможность клиенту свободно выбирать поставщика сетевых услуг и не привязываться к определенному телекоммуникационному оператору. Благодаря используемым подходам в случае потери связи восстановление соединения через новый канал произойдет автоматически в течение одной минуты.

Взаимодействие проходит в защищённом виде только через открытые интернет-каналы с применением ноу-хау в области обработки финансовых сообщений.

«КиберПлат» в качестве основного сетевого транспортного механизма использует в своих решениях метод передачи данных через HTTPS. Все передаваемые сообщения подписываются электронными подписями.

Этот механизм предоставляет клиентам и провайдерам CyberFT возможность подключения без выполнения сложных действий, связанных с настройкой сетевого оборудования. В частности, такой способ соединения позволяет подключаться к сети CyberFT через любой прокси-сервер.

На стороне контрагента не требуется дополнительных сетевых устройств и в большинстве случаев изменений в политике сетевой безопасности. Отсутствие дополнительных согласований и инженерных работ обеспечивает высокую скорость подключения и делает его доступным для всех желающих.

За 20 лет эксплуатации системы «КиберПлат» (CyberPlat®) через открытые каналы с применением методов программного шифрования было передано более 12 миллиардов сообщений без единого случая взлома, поэтому и в CyberFT взаимодействие между клиентом и процессингом осуществляется по любым интернет-каналам без специальной аппаратуры. Использование исключительно программного шифрования и применение любых каналов связи резко удешевляют подключение к сети CyberFT. Компания «КиберПлат», провайдер CyberFT, не взимает плату за подключение, и программное обеспечение также предоставляется бесплатно.



При необходимости для подключения могут быть использованы и выделенные каналы связи. Например, по ним могут проходить платежи на значительные суммы между особо крупными клиентами. Разработчик платформы CyberFT рекомендует следующее параметры оценки.

- Если в сутки объём платежей составляет до \$1 миллиона, то необходимость в выделенном канале отсутствует.
- Если объём платежей находится в диапазоне от \$1 до \$20 миллионов в день, то потребность в выделенном канале определяется на усмотрение контрагента.
- При объёме платежей, превышающим сумму в \$20 миллионов в день или для операций, критичных по времени (Forex, операции на фондовом рынке и т.д.), выделенный канал рекомендован. В этом случае соединение через публичный интернет будет использоваться как резервный канал связи.

В системе CyberFT используются сменные (подключаемые) системы криптографической защиты информации (СКЗИ), в том числе OpenSSL и алгоритмы ГОСТ (на основе CryptoPro, Signal-COM и др.). Кроме того, компания «КиберПлат» по требованиям клиентов готова подключать любые другие средства криптозащиты в самые сжатые сроки — в течение нескольких дней.

КОНКУРЕНТОСПОСОБНОСТЬ

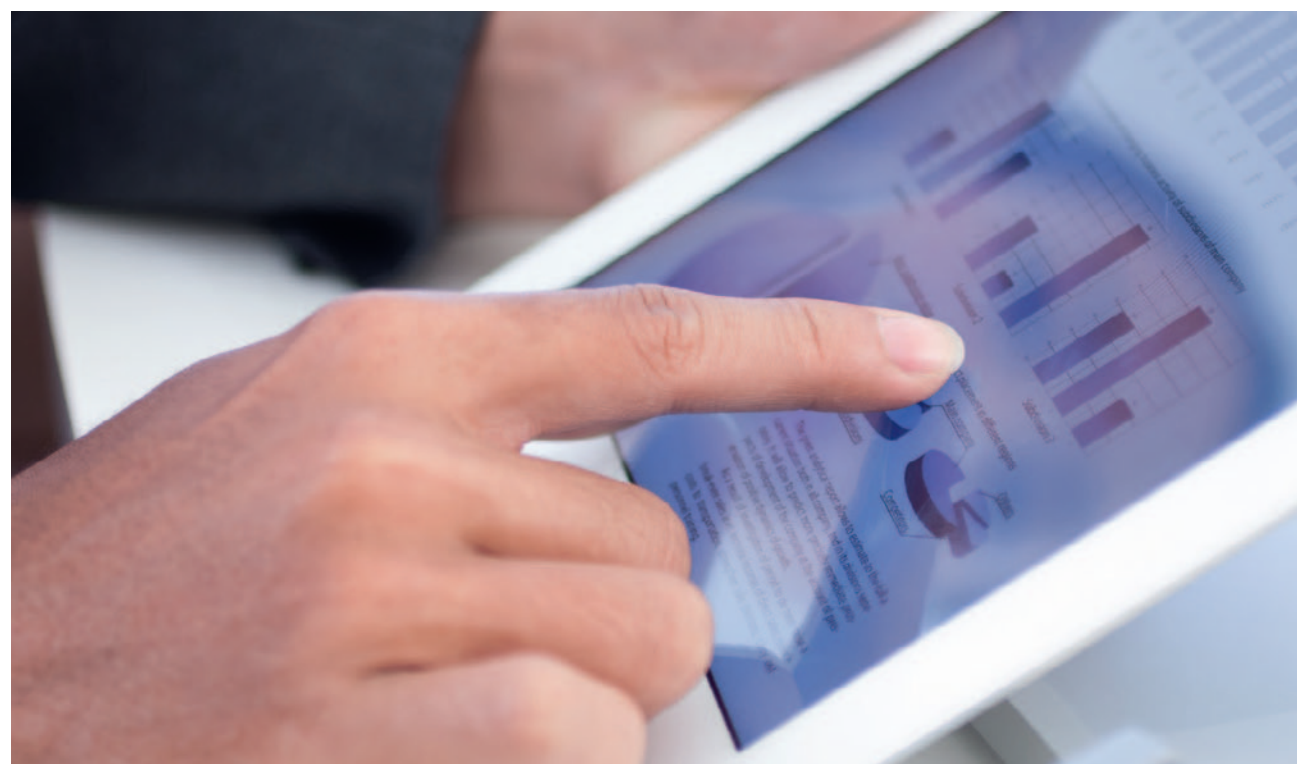
Для клиента работа в сети CyberFT более эффективна и экономически выгодна, чем использование зарубежного аналога — системы SWIFT.

Передача сообщений в сети CyberFT у провайдера «КиберПлат» обходится в два раза дешевле по сравнению с передачей подобных сообщений в международной системе SWIFT. При этом плата за подключение к сети CyberFT и комиссия за обслуживание отсутствуют.

Более того, в отличие от SWIFT в системе CyberFT не взимаются комиссии за такие дополнительные услуги, как предоставление данных из архива или, например, присвоение участнику идентификатора и включение его в централизованный справочник.

С клиентской частью CyberFT может работать неограниченное количество пользователей, и плата за дополнительные автоматизированные рабочие места отсутствует. Модуль для интеграции с учётными банковскими системами поставляется также бесплатно в рамках клиентского ПО CyberFT.

Аппаратные требования к работе в CyberFT значительно ниже тех, которые выдвигает SWIFT, поэтому использование платформы позволит снизить затраты на содержание серверного и телекоммуникационного оборудования, а также расходы на персонал, обслуживающий оборудование.



ТЕКУЩАЯ СИТУАЦИЯ С РАСЧЁТАМИ В РФ

Существующая сегодня в России система расчётов не в полной мере обеспечивает потребности экономики в своевременных платежах. Для того чтобы проиллюстрировать данное утверждение, достаточно сравнить существующие параметры платежей, проходящих через Межрегиональный центр обработки информации (МЦОИ) Банка России, с опытом других стран.

Величина (ёмкость) рынка

По неофициальной информации, ежегодно Банк России обрабатывает 600 миллионов платежей коммерческих банков на общую сумму 900 триллионов рублей. До 80% от общего количества платежей (400 миллионов) составляют расчёты на суммы, не превышающие 100 тысяч рублей. Суммарно эти платежи составляют менее одного процента от общего оборота (всего 6 триллионов рублей).

Стоимость проведения платежей в Центре межбанковских расчётов Национального Банка Республики Казахстан, приведенная в тенге и рублях

Время проведения платежа	Стоимость, тенге	Стоимость, руб.
с 16:00 до 9:00	9	2,8
с 9:00 до 13:00	11	3,4
с 13:00 до 16:00	22	6,8

Стоимость платежей для банков

Минимальная стоимость платежа для банков составляет 7 рублей, средняя стоимость платежа — 12 рублей. Общие затраты банков на оплату услуг МЦОИ Банка России по мелким платежам составляют 4,8 миллиардов рублей, а по самым минимальным оценкам — 2,8 миллиардов рублей. Снижение этой цифры благоприятно отразится на структуре расходов банков, а значит, увеличит стабильность банковской системы в целом.

- В настоящий момент стоимость платежа через МЦОИ Банка России составляет:
- от 7 до 24 рублей при порейсовой обработке, время проведения платежа — от одного до нескольких часов;
 - 25 или 30 рублей в случае онлайн-ового БЭСП (не работает ночью и в выходные).

Несомненно, действующие тарифы являются завышенными и потенциально могут быть сокращены в несколько раз — это доказывает стоимость аналогичных услуг в сопредельных странах.

Рассмотрим, например, тарификацию аналогичных услуг в Центре межбанковских расчётов Национального Банка Республики Казахстан. При этом все расчёты между банками в Казахстане идут в режиме реального времени и занимают не более нескольких минут.

Таким образом, стоимость срочного платежа в России в 3,6 (!) раза превышает самый дорогой платёж в Казахстане. Обработка всех платежей в Центре межбанковских расчётов занимает несколько минут, а в РФ доходит до 9 часов.

Очевидно, это происходит потому, что в России в настоящий момент не существует полноценной системы онлайн-овых межбанковских расчётов.

Необходимо отметить, что создание постоянно действующей системы обработки небольших безналичных платежей стало не только необходимым, но и практически осуществимым. Развитие технологий приводит к тому, что стоимость обработки платежа может быть существенно снижена и доведена до размеров, при которых она станет доступной для всех без исключения участников рынка (по нашим расчётам, не более 1 рубля за платёж).

Экономия для банков составит в среднем 4,4 миллиарда рублей, по самым консервативным прогнозам не менее 2,4 миллиарда. При этом следует иметь в виду, что обработка относительно небольших платежей влечёт гораздо меньшие риски и, следовательно, требует меньших усилий с точки зрения организации физической безопасности и контроля расчётов. Это обстоятельство позволяет обособить данный вид расчётов в рамках отдельной системы, которая должна быть, с одной стороны, надёжной, а с другой — окупаемой и экономически выгодной участникам.

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Платформа CyberFT разработана для массового использования участниками рынка, поэтому требует минимальных системных характеристик: для работы пользователей достаточно обычной рабочей станции и веб-браузера.

Требования к программному обеспечению терминала CyberFT:

- Debian GNU / Linux 7.6 (wheezy) Release: 7.6;
- файловая система ext3 или ext4;
- возможна установка ПО на виртуальную машину!

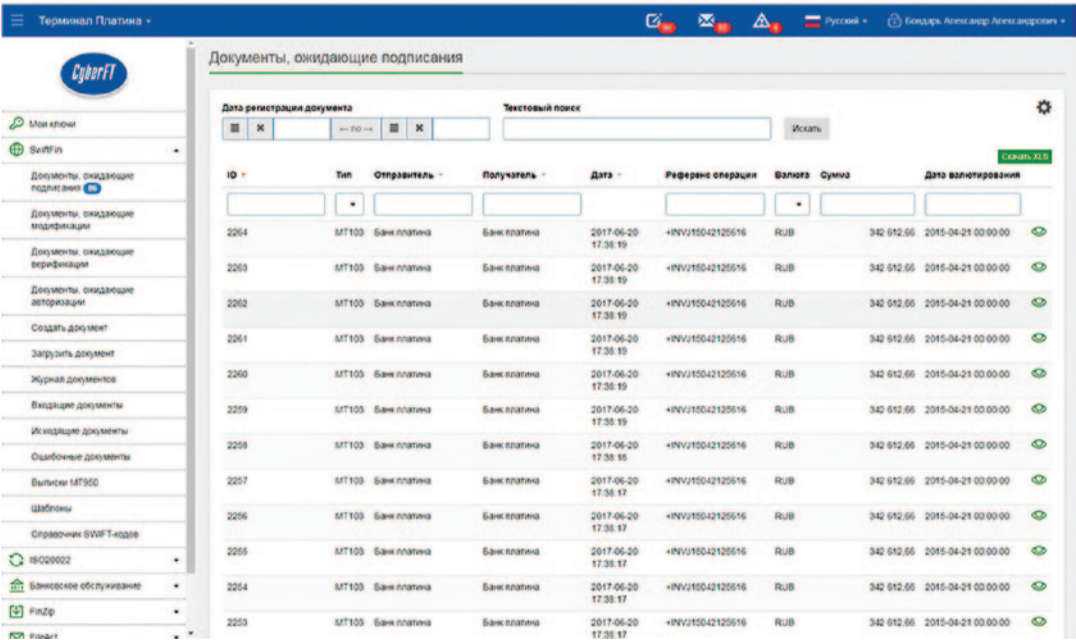
Требования к аппаратному обеспечению терминала CyberFT:

- архитектура процессора x86-64;
- объём ОЗУ не менее 4Gb;
- многоядерный ЦП уровня Intel Core 2 Duo 3.0 Ghz и выше;
- объём жёсткого диска не менее 40Gb.

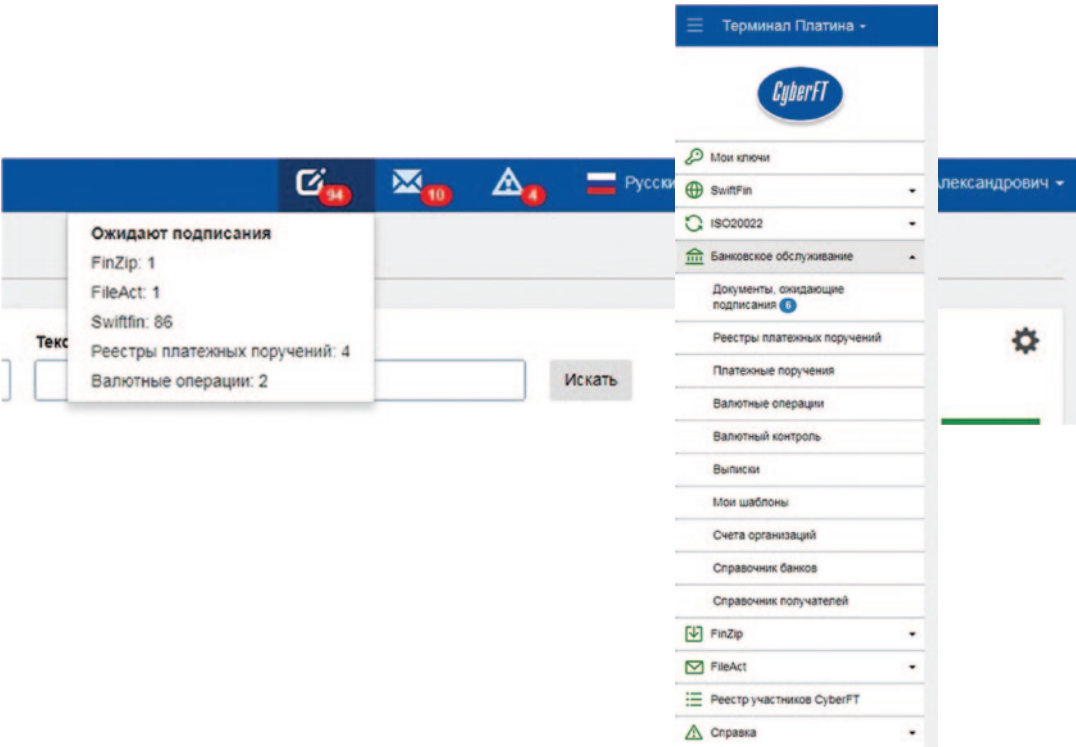
ТЕРМИНАЛ CYBERFT



Главное меню



Журнал документов



Работа с документами



* Терминал CyberFT может быть установлен в виде приложения на стороне клиента, либо доступен в качестве «тонкого» клиента

Схема работы через терминал

CYBERFT: ОДНА СИСТЕМА ДЛЯ РЕШЕНИЯ МНОЖЕСТВА ЗАДАЧ



УНИВЕРСАЛЬНОЕ РЕШЕНИЕ ДЛЯ ВЗАИМОДЕЙСТВИЯ КОРПОРАТИВНЫХ КЛИЕНТОВ С БАНКАМИ

Холдинговые компании используют классические системы дистанционного обслуживания для управления счетами в различных банках, и в случае крупных размеров холдинга количество расчётных банков может исчисляться десятками. Это приводит к тому, что холдинг вынужден обслуживать одновременно множество систем «Клиент-Банк», что порождает целый ряд сложностей. Требуются дополнительные затраты на персонал для администрирования и поддержки систем «Клиент-Банк» от разных банков, а также на аппаратное и программное обеспечение. Более того, функциональность многих систем «Клиент-Банк» часто не позволяет организовать полноценную дистанционную работу с банком.

Ситуацию не спасает и применение систем уровня «Расчётный центр корпорации» или «Центр финансового контроля» по причине отсутствия универсального механизма работы с разными банками.

Даже прямая интеграция учётной системы клиента с банком (Host-to-Host) полностью не решает задачу, так как каждый банк предлагает клиенту свой канал обмена данными, определённые форматы и определённые средства криптографической защиты информации.

Ограничения при классическом подходе к удалённому управлению счетами

Время проведения платежа	ДБО	РЦК	Классический H2H
Количество установок систем ДБО	Высокое	Среднее	Не требуется
Сложность администрирования	Высокая	Высокая	Средняя
Гибкость	Низкая	Низкая	Средняя
Безопасность	Низкая	Низкая	Средняя
Разнообразие используемой криптографии	Высокое	Среднее	Среднее
Разнообразие форматов обмена данными	Высокое	Среднее	Среднее
Стандартизация	Низкая	Низкая	Средняя
Комиссия за подключение и обслуживание	Высокая	Очень высокая	Средняя

УНИВЕРСАЛЬНЫЙ HOST-TO-HOST

Платформа CyberFT позволяет решить вышеперечисленные проблемы, сократить финансовые и временные затраты на дистанционное банковское обслуживание за счёт полного отказа от систем «Клиент-Банк» и использования единого терминала CyberFT, который предоставляет возможности:

- организовать единый безопасный канал для взаимодействия со всеми расчётными банками;
- использовать единые форматы обмена данными с различными банками;
- легко интегрироваться с учётными системами на стороне клиента различными способами;
- использовать единые средства криптографической защиты информации при работе с различными банками;
- получить дополнительные опции дистанционного банковского обслуживания, недоступные при работе через стандартные системы «Клиент-Банк»;
- использовать ключи подписи (усиленная квалифицированная подпись), полученные в аккредитованном удостоверяющем центре.

В настоящее время сервис широко используют для взаимодействия с обслуживаемыми банками юридические лица — клиенты банка, а также компании, входящие в состав одного из крупнейших холдингов — ЕВРАЗ.

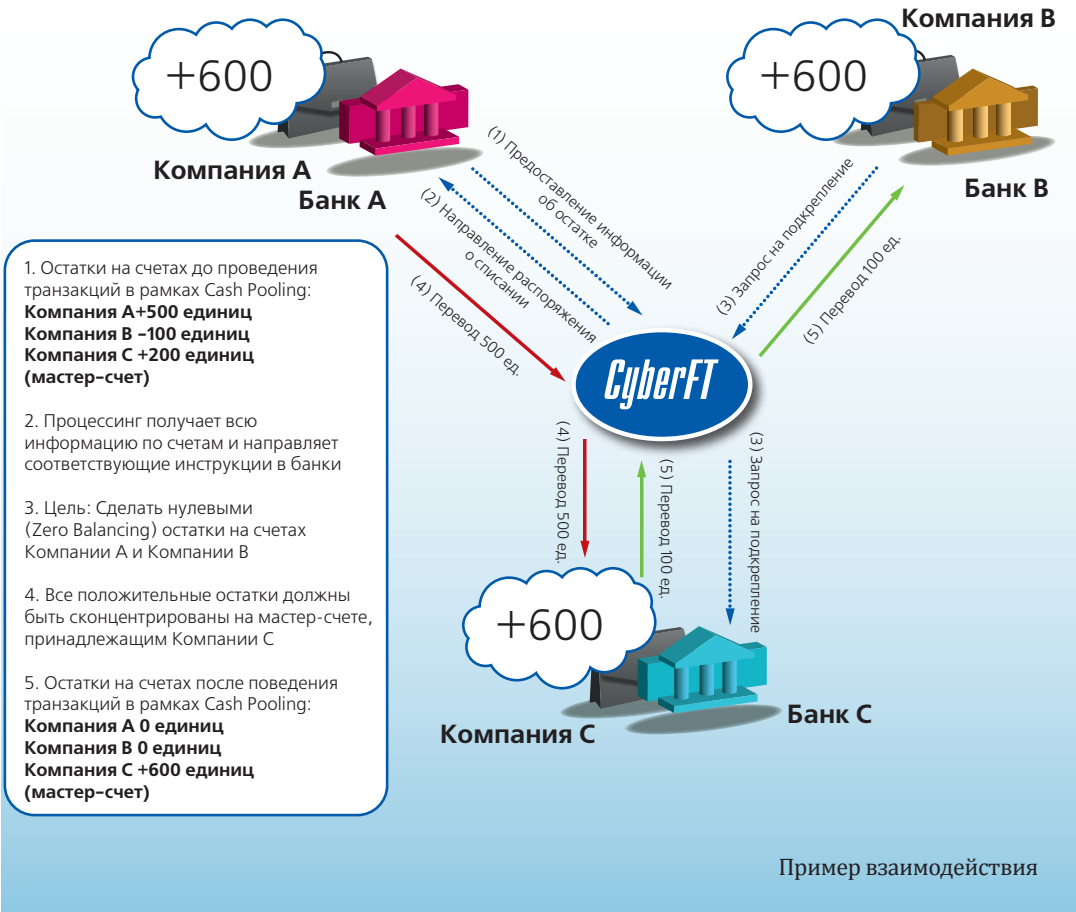


МЕЖБАНКОВСКИЙ CASH POOLING

Система CyberFT позволяет организовать межбанковский Cash Pooling, лишённый наиболее важного недостатка — привязки счетов к конкретному банку.

Роль расчётного центра, которую обычно играет автоматизированная банковская система внутри одного банка, выполняет процессинг CyberFT. Таким образом, корпоративные клиенты получают широкие возможности для организации автоматических межбанковских переводов в рамках холдинга или группы компаний.

В свою очередь, банки, которые на текущий момент не предоставляют Cash Pooling либо желают расширить его функциональность без существенных доработок, смогут использовать для этих целей возможности CyberFT.



ПЛАТЁЖНЫЙ МОДУЛЬ CYBERFT 1С

Платёжный модуль CyberFT 1С позволяет клиентам из интерфейса системы 1С создавать, подписывать и отправлять в банк различные платёжные документы, включая рублевые и валютные переводы, заявки на покупку и продажу валюты, документы валютного контроля и др., а также принимать из банка выписки, сообщения и информацию по статусам отправленных документов.

CyberFT 1С обеспечивает взаимодействие с банками напрямую, без использования таких «промежуточных звеньев», как системы «Клиент-Банк». Это существенно сокращает время на подготовку и отправку в банки документов, снижает операционные издержки и риски, связанные с ошибками при подготовке и верификации исходящих документов.



Основные преимущества платёжного модуля CyberFT 1С

- Совместимость с «1С:Бухгалтерия предприятия 3.0» и платформой «1С:Предприятие 8.3».
- «Толстая» и «тонкая» версии.
- Универсальная и полноценная замена всех систем «Клиент-Банк».
- Высокий уровень безопасности.
- Поддержка основных типов документов, необходимых для работы с банками.
- Поддержка CryptoPro и e-Token.
- Возможность работы с разными банками.
- Различные варианты интеграции с банками.
- Работа со списком доверенных получателей.
- Управление правами пользователей.
- Подписание документов непосредственно в 1С.

СХЕМА РАБОТЫ

Вариант 1



Вариант 2

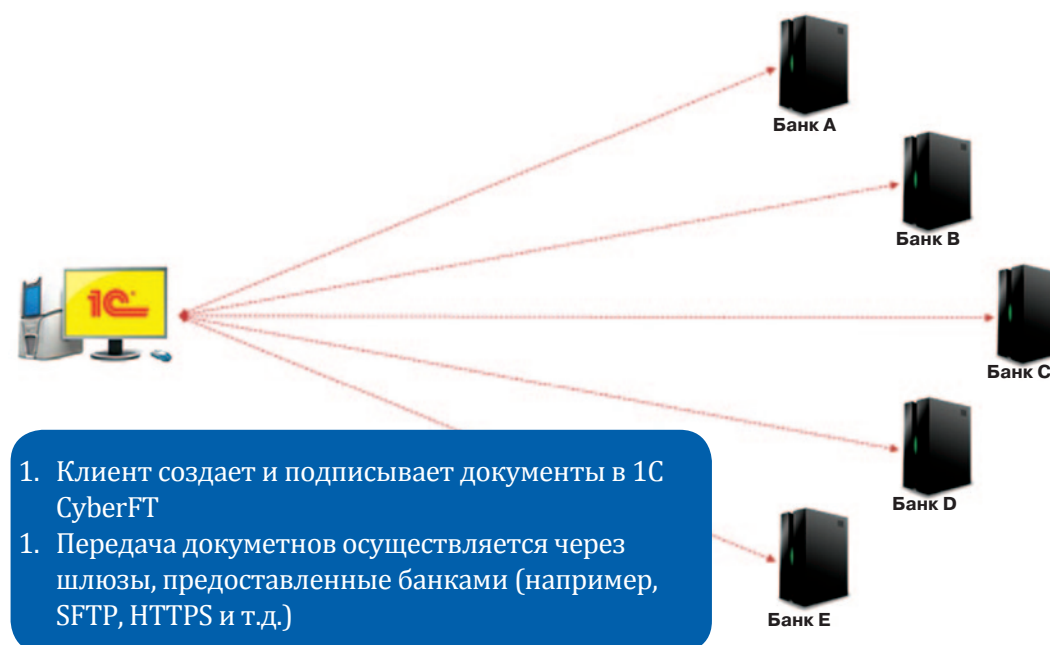


СХЕМА РАБОТЫ ЧЕРЕЗ ERP

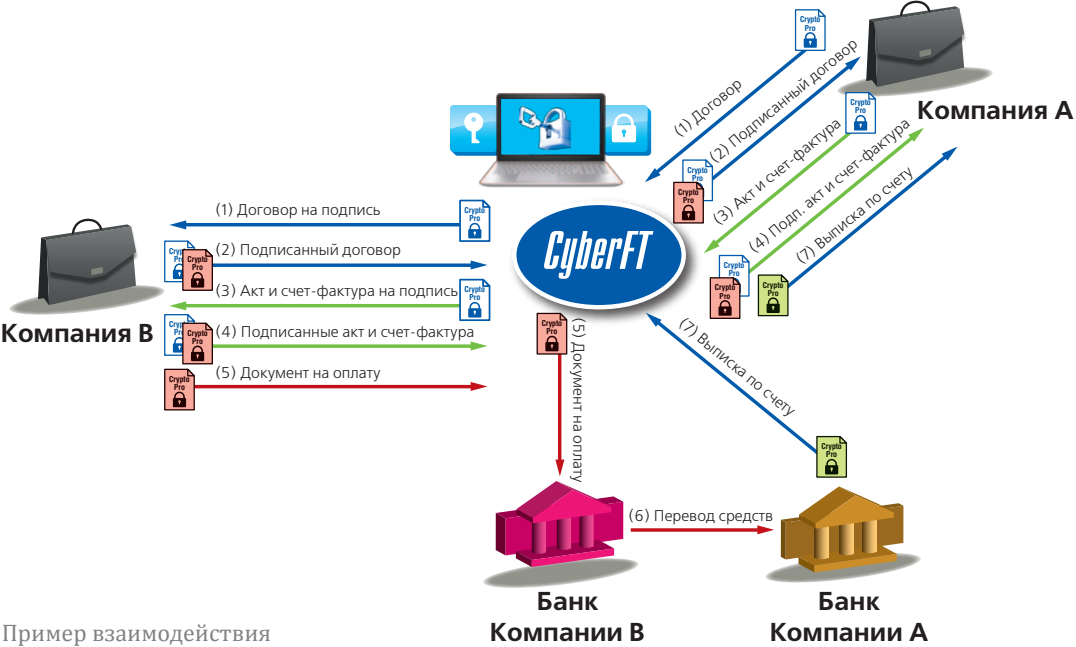


ЮРИДИЧЕСКИ ЗНАЧИМЫЙ МЕЖКОРПОРАТИВНЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Компании могут взаимодействовать через CyberFT не только с банками, но и друг с другом, организовав электронный документооборот юридически значимых документов. Например, два участника, установив между собой доверительные отношения, могут обмениваться в электронной форме контрактами, счетами (инвойсами) и другой информацией, необходимой для ведения бизнеса.

Также на базе CyberFT при участии банков можно построить систему электронного выставления и оплаты счетов (e-Invoicing) и межбанковского прямого дебетования (Direct Debit), когда средства будут списываться с получателей услуг в пользу провайдера услуги автоматически на основании заранее данного акцепта.

Несмотря на множество существующих на рынке систем электронного документооборота, CyberFT позволяет охватить всех корпоративных клиентов и все банки не только на территории России, но и за её пределами. При этом Терминал CyberFT может быть интегрирован с локальной системой электронного документооборота, функционирующей на стороне компании.



ОСНОВНЫЕ ПРЕИМУЩЕСТВА CYBERFT

- Оптимизация затрат, связанных с проведением финансовых транзакций и обменом документами с контрагентами.
- Высокие стандарты безопасности и гарантия сохранности передаваемой информации, в том числе содержащей коммерческую тайну.
- Полное соответствие законодательству при проведении финансовых операций.
- Быстрое и низкозатратное внедрение и развертывание.
- Различные варианты подключения, учитывающие особенности работы организации и требования к уровню безопасности.
- Доступность 24×7.
- Абсолютная независимость от внешнеполитической ситуации.
- Высокая отказоустойчивость работы системы.
- Проведение транзакций в режиме онлайн.
- Поддержка современных форматов обмена данными, включая SWIFT InterAct, SWIFT FileAct и SWIFT Fin (все документы категории MT).
- Гибкость и масштабируемость системы как в области форматов обмена данными, так и в области интеграции с криптографическими библиотеками и поддержки каналов передачи данных.
- Многовариантность использования системы: от закрытой группы банков до взаимодействия на международном уровне.
- Возможность создавать целый спектр новых сервисов для клиентов банков.
- Мгновенное проведение финансовых транзакций.
- Возможность проведения финансовых операций вне рамок операционного дня.
- Электронный документооборот юридически значимых документов для клиентов банка.
- Интеграция с ERP, учётной или бухгалтерской системой клиента и построение универсального Host-to-Host решения.
- Возможность для корпоративных клиентов перехода на единый канал взаимодействия с банками (Host-to-Host) и отказа от использования традиционных систем «Клиент-Банк».
- Возможность организации межбанковского физического Cash Pooling и многое другое.



ЭФФЕКТ ОТ ВНЕДРЕНИЯ CYBERFT

Ожидаемые эффекты от внедрения системы в первую очередь проявятся в охвате розничного банковского рынка и сегмента малого и среднего бизнеса. Кроме того, CyberFT позволяет создать площадку, которая будет способствовать укрупнению размеров платежей и выходу на принципиально новый уровень расчётов.

Для розничного банковского рынка

Развитие рынка розничных банковских услуг достигло того уровня, когда для эффективной конкуренции банкам необходимо предоставлять своим клиентам максимально возможный уровень сервиса. Например, держатели кредитов ожидают, что внесение наличных средств любым удобным для них способом мгновенно снимет с них требования со стороны банка. Вкладчики предпочитают работать с банками, в которых положенные на депозит средства моментально оказываются на счёте.

Таким образом, система, отвечающая современным требованиям оперативности зачисления денег при разумных расходах на операцию, сразу станет востребованной.

Когда будет решена проблема выдачи сдачи конечному пользователю при осуществлении расчётов между банками, Банк России окажет поддержку развитию этого сегмента платёжной системы.

Для рынка малого и среднего бизнеса

Одна из основных проблем развития малого бизнеса состоит в отсутствии каких бы то ни было лимитов на контрагента. При этом уровень доверия контрагентов друг к другу при купле-продаже товаров или потребительских услуг крайне низок, особенно в регионах. Риск потери активов и прибыли для малого бизнеса крайне высок, ведь недобросовестное поведение контрагента может поставить под удар само существование бизнеса.

Например, машина с зерном стоит на элеваторе до тех пор, пока элеватор не получит деньги за отгруженный товар. И даже если платёж отправлен до прибытия машины, порейсовая обработка может занять несколько часов, а это несколько часов рабочего времени водителя. Более того, срыв сроков поставки зерна даже на считанные часы может сказаться на работе всего мукомольного комбината или хлебопекарни.

Одной из проблем розничной и мелкооптовой торговли является невозможность осуществления безналичных платежей в течение всего времени работы торговых точек, то есть круглосуточно, семь дней в неделю. Накапливающаяся в течение выходных дней торговая выручка не может быть использована для оплаты новых мелкооптовых поставок товаров, необходимых для поддержания ассортимента.

При отсутствии достаточного доверия между оптовыми поставщиками и розничными торговцами первые ожидают оплату до отгрузки товара, а последние зачастую не готовы авансировать крупные суммы до поставки. Эта проблема особенно обостряется в периоды праздников, когда объективно увеличивается торговый оборот, а количество дней банковских каникул возрастает. Для поддержания товарооборота торговые точки вынуждены заранее обращаться

за кредитом в банки с целью наращивания товарных запасов. Однако взятие кредита не всегда возможно и достаточно дорого, а накопление товарных остатков неприемлемо при реализации скоропортящейся продукции.

Проблема доверия давно решена в расчётах розничных магазинов с покупателями — физическими лицами. Платёжи производятся наличными деньгами или в безналичном порядке с помощью кредитных карт. На практике расчёты между розничными точками (особенно небольшими) и поставщиками также имеют тенденцию к переходу на наличные. При этом наличные денежные средства доверяются неспециализированным лицам (водителям, экспедиторам). Такое положение объективно сдерживает развитие безналичных расчётов, порождая криминальные риски и создавая почву для злоупотреблений с неучтённой наличностью.

Платформа CyberFT, кроме решения множества других насущных задач, позволяет высокоэффективно справиться и с решением описанной проблемы розничных сетей, ускорить оборачиваемость средств и привести к увеличению розничного товарооборота на 5–7%.

ПЛАТФОРМА CYBERFT ДЛЯ ОРГАНОВ ВЛАСТИ, ВЕДОМСТВ, ГОСУДАРСТВЕННЫХ И ЧАСТНЫХ КОМПАНИЙ

ТЕКУЩАЯ СИТУАЦИЯ СО ВНУТРИ- И МЕЖВЕДОМСТВЕННЫМ ДОКУМЕНТООБОРОТОМ В РОССИИ

В настоящее время вопрос межведомственного электронного взаимодействия внутри РФ не имеет централизованного решения, т.к. МЭДО (Межведомственный Электронный Документооборот (Постановление Правительства РФ об утверждении положения о МЭДО №754 от 22.09.2009)), оператором которого будет ФСО, еще находится в стадии создания (только согласован стандарт сообщений – PDF/A) – и в настоящее время осуществляется тестовая эксплуатация с участием Минпромторга, Минэкономразвития и еще двух-трех структур. При этом МЭДО фактически представляет собой только защищенную межведомственную электронную почту. Вопрос же интеграции с разнородными системами ЭДО, используемыми в различных организациях (хотя бы на уровне поддержания согласованного формата) пока находится в стадии обсуждения. Помимо сложностей с интеграцией на этапе тестовой эксплуатации были выявлены существенные технологические ограничения, в частности, невозможность передачи больших объемов информации в одном сообщении (свыше 0,5Mb).

Отсутствие работоспособного МЭДО не позволяет ведомствам и организациям обеспечивать выполнение требований указанного постановления при организации информационного обмена служебной информацией, имеющей высокую коммерческую ценность или грифы секретности. Общедоступные почтовые сервисы, которые используются в таких случаях, кратно увеличивают риски утраты служебной информации и запрещены к использованию компетентными органами при передаче данных, содержащих гостайну.

Зачастую государственные структуры и иные организации для отправки секретной информации вынуждены прибегать к услугам фельдъегерской службы. Такой метод передачи особо важных данных резко тормозит процесс принятия ответственных решений, а также значительно удорожает процесс обмена информацией.

Разрешённые к использованию системы передачи секретных данных на текущий момент, во-первых, недостаточно распространены, во-вторых, не позволяют передавать большой объём информации, напимер, карты или телеметрию. Кроме того, они основаны на аппаратной защите данных, а это уже не соответствует текущим рискам и несёт значительные угрозы дешифровки злоумышленниками перехваченных сообщений.



Локальные решения взаимодействующих между собой госструктур базируются на порталных решениях и не выдерживают никакой критики с точки зрения уровня безопасности. Подобные порталные решения достаточно часто защищены лишь паролем пользователя и, к сожалению, не поддерживают электронной подписи и, соответственно, не могут служить для обмена юридически значимыми документами. Более того, применение порталных технологий не позволяет использовать эти решения для автоматизированных межведомственных взаимодействий. Присегоднешнем объёме межведомственных коммуникаций сложно представить, что каждое сообщение для коммуникации между ведомствами будет введено в веб-интерфейсе портала, поэтому очевидна необходимость использования интегрированного решения для взаимодействия существующих информационных систем ведомств.

Единая система межведомственного электронного взаимодействия (СМЭВ) работает с 2013 года, содержит 83 региональных узла и центральный узел, более 600 участников, 7 ЦОДов, оператор — Ростелеком). СМЭВ (согласно Федеральному закону от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг») представляет собой, по сути, шину данных, к которой подключены учётные системы и системы ЭДО участников. В связи с тем что SOA-архитектура системы реализована на базе 84 шин Oracle ESB, вопрос безопасности данного решения также вызывает серьёзные сомнения.

ПЛАТФОРМА CYBERFT — ЭЛЕМЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ГАРАНТ СОХРАННОСТИ ВАЖНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИИ

В создавшейся ситуации очевидно, что государственные и коммерческие структуры страны остро нуждаются в современной онлайн-системе обмена информацией, способной стать основой защищённого документооборота любой степени секретности.

Эта система должна быть:

- относительно простой;
- недорогой;
- быстродействующей;
- легко масштабируемой;
- обладать высокой пропускной способностью;
- основываться не на аппаратных, а на программных методах защиты данных с возможностью быстрой смены криптобиблиотек.

Данным критериям полностью соответствует платформа CyberFT, которая позволяет государственным структурам и другим участникам документооборота:

- осуществлять информационный обмен в полном соответствии с локальным законодательством;
- полностью защищать передаваемую информацию от внешнеполитических угроз;
- гарантировать сохранность информации, содержащей государственную и коммерческую тайну;

- организовать электронный документооборот юридически значимых документов между органами государственной власти и другими участниками;
- оптимизировать затраты и повысить скорость передачи информации.



Говоря простым языком, платформу CyberFT можно представить аналогом сети интернет. Однако принципиальными отличиями CyberFT от Всемирной паутины являются гарантированная идентификация участников и обмен структурированной информацией в зашифрованном виде.

До выступлений Эдварда Сноудена и Джулиана Ассанжа о массовой слежке и утечке информации не все госструктуры точно представляли уровень радиотехнической и компьютерной разведки развитых стран и частных разведывательных компаний, недостаточно задумывались над опасностью недружественного воздействия на обмен данными, содержащими конфиденциальную информацию.

Применение платформы CyberFT является эффективным способом для реализации защищённого и юридически значимого взаимодействия между органами власти, министерствами и ведомствами страны как между собой, так и с коммерческими, общественными и другими организациями.

CyberFT позволяет объединить в сеть неограниченное число ведомств, являющихся организаторами информационного обмена (провайдерами CyberFT). Платформа CyberFT разворачивается на площадке провайдера и является независимой от её разработчика — компании «КиберПлат».

Провайдер CyberFT может обслуживать все свои структуры и их контрагентов в регионах присутствия либо работать внутри отдельно выбранных подконтрольных ведомству организаций или их групп.

Ведомства могут соединяться друг с другом через межплатформенную связь, контролируемую ответственным сотрудником ведомства, который дает пользователям из одного ведомства право переписки с другим ведомством.

В отличие от других систем, работающих на мировом рынке, всё программное обеспечение разработано российскими специалистами (обладает лицензионной и патентной независимостью). Все серверы платформы CyberFT будут располагаться в защищённом периметре провайдера, поэтому вероятность утечки государственных и важных коммерческих данных в электронном документообороте резко уменьшается.

ИНСТРУМЕНТ ИСПОЛНЕНИЯ ЛОКАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Для органов власти CyberFT представляет собой программную платформу, реализующую защищённую информационную магистраль передачи всех общепринятых типов сообщений внутриведомственного, финансового и коммерческого электронного документооборота, функционирующего в соответствии с приказом Минкомсвязи и Федеральной службы охраны (ФСО) от 22 сентября 2015 года «Об утверждении требований к организационно-техническому взаимодействию госорганов и госорганизаций посредством обмена документами в электронном виде» и соответствующего ряду требований:

- к форматам файла электронного документа, а также файлам электронного образа документа, поддерживающих передачу электронных документов в виде файлов произвольного формата, в том числе формата PDF/A-1, определяемым международным стандартом ISO 19005-1:2005, а также ISO 20015 и ISO 20022;
- к усиленной квалифицированной электронной подписи, с использованием специализированного формата PKCS#7;
- к транспортным контейнерам и возможности преобразования контейнеров из одного вида представления в другой в процессе создания, обработки и хранения документов.

СРЕДСТВО БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ОБМЕНА

Решение CyberFT предполагает, что для документов уровня секретности «ДСП» и «С» могут быть использованы как выделенные каналы связи, так и открытые каналы интернет. При этом технология обеспечивает создание зашифрованного канала между точками обмена сообщениями. По этим каналам передаются зашифрованные сообщения, подписанные электронной подписью.

Основной объём передаваемой информации может проходить в защищённом виде через открытые интернет-каналы и/или выделенные каналы ведомства с применением ноу-хау в области обработки защищённых сообщений.

Компания «КиберПлат» в качестве основного сетевого транспортного механизма использует в своих решениях метод передачи данных, где все передаваемые сообщения подписываются юридически значимыми электронными подписями и передаются по сети в криптоконтейнерах с длиной ключа 2048 внутри SSL-туннеля.

Рекомендации по использованию интернета, VPN и выделенных каналов связи

	«ДСП»	«С»
Интернет	Да	При аварии более защищённого типа соединения и жёсткой необходимости срочно передать сообщение
VPN	Можно, но не обязательно	Да
Выделенный канал или особо защищённая линия	Можно, но не обязательно	Можно, но не обязательно

ОСНОВНЫЕ СТРАТЕГИЧЕСКИЕ ПРИНЦИПЫ И ВОЗМОЖНОСТИ СЕТИ CYBERFT

Платформа CyberFT представляет собой удобное и абсолютно безопасное решение, реализованное на следующих принципах:

- суверенность;
- бесперебойность;
- безопасность;
- идентификация каждого пользователя;
- структурированность передаваемых данных;
- совместимость;
- универсальность;
- доступность;
- расширяемость.

Платформа CyberFT обеспечивает:

1. Построение безопасной и надёжной системы электронного взаимодействия и документооборота.
2. Передачу сообщений в режиме онлайн — эквивалент закрытой юридически значимой электронной почты с подтверждением получения.
3. Передачу данных в полном соответствии с федеральными, локальными и ведомственными нормативными актами с использованием сертифицированных средств СКЗИ:
 - шифрование сообщений и подписание электронными подписями (ЭП);
 - поддержка сменных СКЗИ, сертифицированных надлежащими государственными органами, включая OpenSSL, CryptoPro, SignalCOM, Агава и др., а также поддержка усиленной квалифицированной электронной подписи в соответствии с требованиями Федерального закона № 63-ФЗ «Об электронной подписи»;
 - использование протоколов HTTPS (TLS-туннель) при передаче данных;
 - поддержка VPN и выделенных каналов связи;
 - возможность передачи программно зашифрованных сообщений через каналы открытого интернета с использованием зашифрованных туннелей, не допускающих дешифрацию, для случаев аварийной недоступности выделенных каналов.
4. Использование современных стандартов, нормативных требований и возможность настройки собственных форматов сообщений, а также порядка обмена и обработки.



ОТЛИЧИТЕЛЬНЫЕ ПРИЗНАКИ СЕТИ CYBERFT

Многопровайдерность

Платформа CyberFT для органов власти, ведомств, государственных и частных компаний разворачивается на площадке провайдера и является независимой от компании «КиберПлат». Провайдер CyberFT может обслуживать или работать внутри отдельно выбранной государственной структуры.

Провайдерами и участниками CyberFT могут выступать как органы государственной власти, так и другие организации. Каждому участнику присваивается уникальный идентификатор сети CyberFT.

Справочник участников сети доступен каждому участнику и обновляется централизованно в автоматическом режиме. Идентификатор является уникальным в рамках не только одного провайдера, но и всей сети CyberFT. Таким образом, участник с определённым идентификатором может быть подключён только к одному провайдеру, что обеспечивает целостность сети.

Информация о прохождении каждого сообщения логируется на стороне каждого провайдера, участвующего в его передаче. Более того, сами сообщения вместе с электронными подписями отправителя хранятся на стороне отправителя, получателя и провайдера в течение неограниченного срока. (На стороне провайдера все сообщения хранятся в зашифрованном виде, и их содержимое недоступно провайдеру.) Таким образом, каждый участник обмена информацией для каждой операции имеет полноценные юридически значимые электронные документы.

Провайдеры CyberFT могут соединяться между собой различными способами, исходя из сложности организационных процессов установления отношений между провайдерами. Некоторые схемы представлены далее.

1. Каждый с каждым



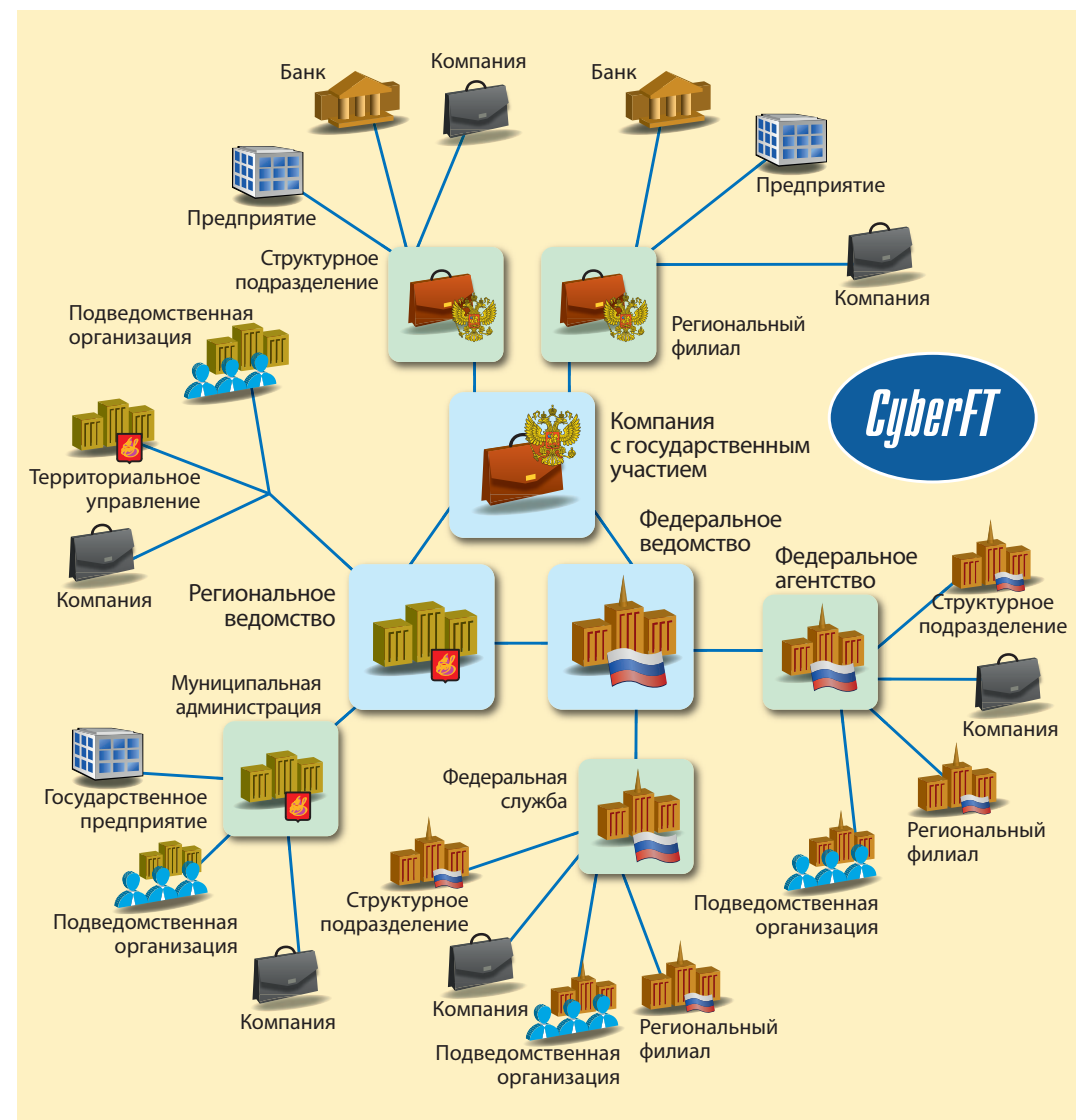
2. Через централизованного провайдера CyberFT, выбранного совместно



Например, любое крупное ведомство или государственная структура могут стать провайдером CyberFT и подключить территориально удаленные подразделения, дочерние организации и других участников своего документооборота. Для обмена данными между участниками, подключёнными к разным провайдерам, эти провайдеры заключают соглашение с единым провайдером (например, министерством), который отвечает за маршрутизацию сообщений между ними.

С одной стороны, такая топология сети существенно упрощает организационные моменты, связанные с установлением отношений между провайдерами, и позволяет работать через единую организацию (центрального провайдера), которой доверяют все участники. С другой стороны в случае сбоя на стороне центрального провайдера связь между участниками сети будет невозможна.

3. Через группу взаимосвязанных провайдеров CyberFT



Данный вариант топологии сети, несмотря на более сложные организационные процессы установления отношений между провайдерами, обладает повышенной отказоустойчивостью.

В случае технических проблем на стороне одного из центральных провайдеров связь между всеми участниками сети CyberFT сохранится.

Совместимость

Участники сети CyberFT также могут взаимодействовать и с другими контрагентами, подключёнными к другим сетям МЭДО. Один из примеров такого взаимодействия представлен на схеме далее.

Программное обеспечение CyberFT позволяет максимально быстро интегрироваться с большинством используемых в различных ведомствах систем электронного документооборота, поддерживая основные форматы документов, что упрощает процесс загрузки и загрузки документов во внутренние информационные системы участников.

При подключении к CyberFT нового участника централизованный справочник участников будет обновлен дистанционно в автоматическом режиме.

Программное обеспечение CyberFT предоставляется клиентам бесплатно.

Доступность

Подключение к сети CyberFT осуществляется через выделенный канал, VPN или публичный интернет, что предоставляет возможность для клиента свободно выбирать поставщика сетевых услуг и не привязываться к определённому телекоммуникационному оператору. Благодаря используемым подходам в случае потери связи восстановление соединения через новый канал произойдет автоматически в течение одной минуты.

Всё взаимодействие проходит в защищённом виде только через открытые интернет-каналы с применением собственных ноу-хау в области обработки финансовых сообщений. Компания «КиберПлат» в качестве основного сетевого транспортного механизма использует в своих решениях метод передачи данных через HTTPS (TLS-туннель). Все передаваемые сообщения подписываются электронными подписями. Например, по ним могут проходить сообщения уровня «С».

В системе используются сменные (подключаемые) системы криптографической защиты информации (СКЗИ), в том числе OpenSSL и алгоритмы ГОСТ (на основе CryptoPro, Signal-COM и др.) Кроме того, компания «КиберПлат» по требованиям партнёров и клиентов готова подключить любые другие механизмы криптозащиты в самые сжатые сроки в течение нескольких дней.

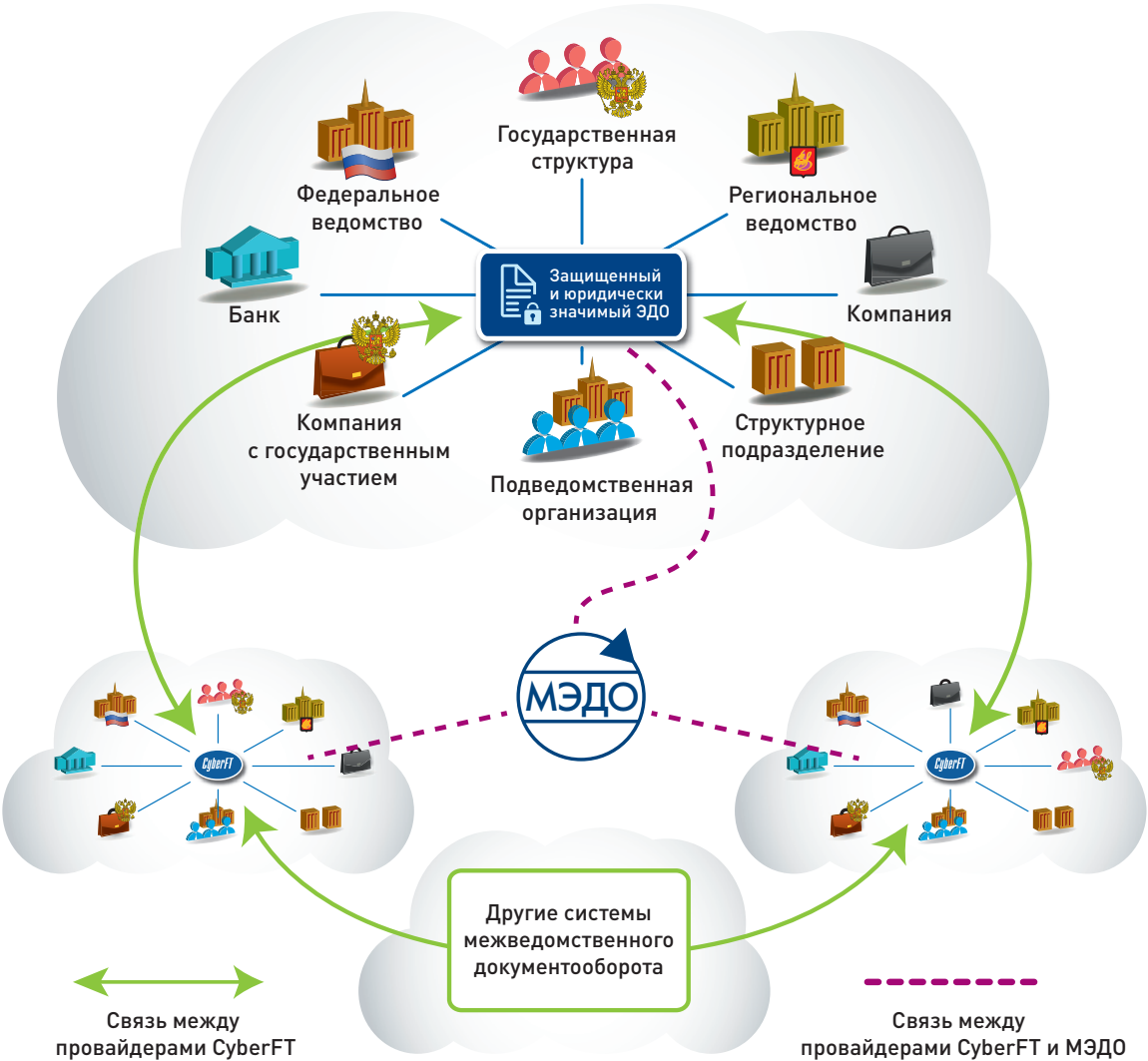
Конкурентоспособность

Принципиальным отличием сети CyberFT от других решений возможных для применения в качестве среды для межведомственного электронного документооборота является её готовность к эксплуатации в настоящий момент, дешевизна и эффективность использования, а также высочайший уровень безопасности и защищённости.

Стоит также отметить, что аппаратные требования к работе в CyberFT значительно ниже тех, которые выдвигают другие разработчики МЭДО, поэтому эксплуатация CyberFT позволяет снизить расходы на содержание серверного и телекоммуникационного оборудования, а также затраты на персонал, обслуживающий данное оборудование.

Универсальность

В рамках универсального транспортного решения в сети CyberFT существует возможность интеграции с большинством используемых в ведомствах систем электронного документооборота. Применение данного подхода позволяет оптимизировать бизнес-процессы, предусматривающие обмен документами с



органами государственной власти (в том числе и взаимодействие с государственной системой СМЭВ), а также межведомственные коммуникации.

Масштабируемость

В CyberFT реализован сервис, позволяющий обмениваться любыми структурированными и неструктурированными сообщениями, а также сообщениями, содержащими вложения. В рамках предлагаемого решения в сети CyberFT существует возможность реализации новых форматов внутри уже имеющихся видов электронных сообщений.

Платформа CyberFT может быть оперативно доработана с учётом потребностей клиентов. В частности, существует возможность быстрого создания новых видов электронных документов при помощи конструктора форматов, что делает платформу CyberFT значительно более гибкой в сравнении с конкурентами.

ЭФФЕКТ ОТ ВНЕДРЕНИЯ

- Возможность эффективной работы в полном соответствии с требованиями законодательства РФ и принятыми стандартами.
- Максимальная надёжность работы и безопасность передаваемой информации.
- Охват большого числа участников межведомственного документооборота.
- Полная независимость от компании-разработчика.
- Отправка и получение зашифрованных сообщений в режиме онлайн.
- Экономия бюджетных средств на инфраструктуре и обслуживании сети.

**«КИБЕРСДАЧА» —
УНИКАЛЬНЫЙ ФИНАНСОВЫЙ
СЕРВИС ДЛЯ РИТЕЙЛА, БАНКОВ,
ПРОВАЙДЕРОВ УСЛУГ**

СУТЬ ПРОДУКТА

«КиберСдача» — современная финансовая технология, связанная с использованием сдачи, оставшейся после оплаты товаров и услуг в розничных сетях, магазинах и мелких торговых точках.

Сумма сдачи может быть в режиме реального времени переведена практически любому поставщику услуг без потери времени кассиром с помощью специальной карты «КиберСдача».

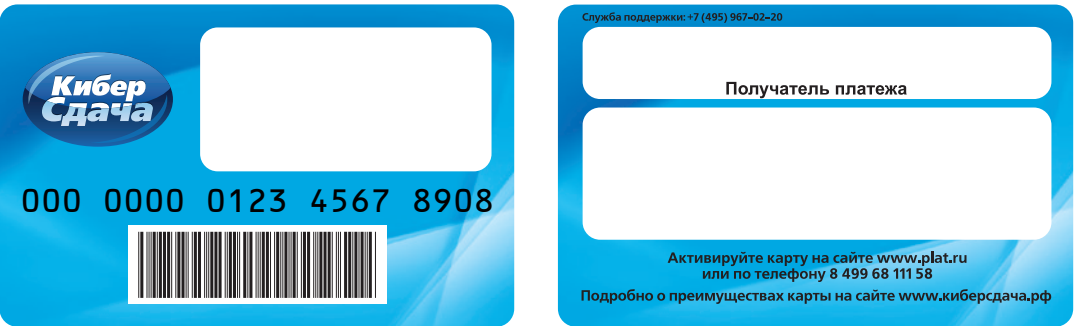
По оценкам экспертов, наблюдается наиболее активный спрос на перевод суммы сдачи на счёт мобильного телефона, банковскую карту, а также расчётный счёт в банке, привязанный к Интернет-Банк-Клиенту, типа «Альфаклик», «Банк в кармане», Plat.ru — Платёжная книжка «КиберПлат».

Пользователем сервиса может стать любой человек. Для реализации сервиса (зачисления сдачи или целевого перевода клиентом средств на банковский или лицевой счёт у провайдера услуг) необходимо взять неактивированную карту и активировать её. В процессе активации номеру карты будет присвоен шаблон, содержащий реквизиты платежа, например, код провайдера услуг и номер мобильного телефона либо код банка и номер банковского или лицевого счёта и номер мобильного телефона. Совокупность данных передаётся в систему «КиберПлат» (CyberPlat®) и в дальнейшем служит электронным шаблоном для осуществления переводов автоматически, без ввода реквизитов.

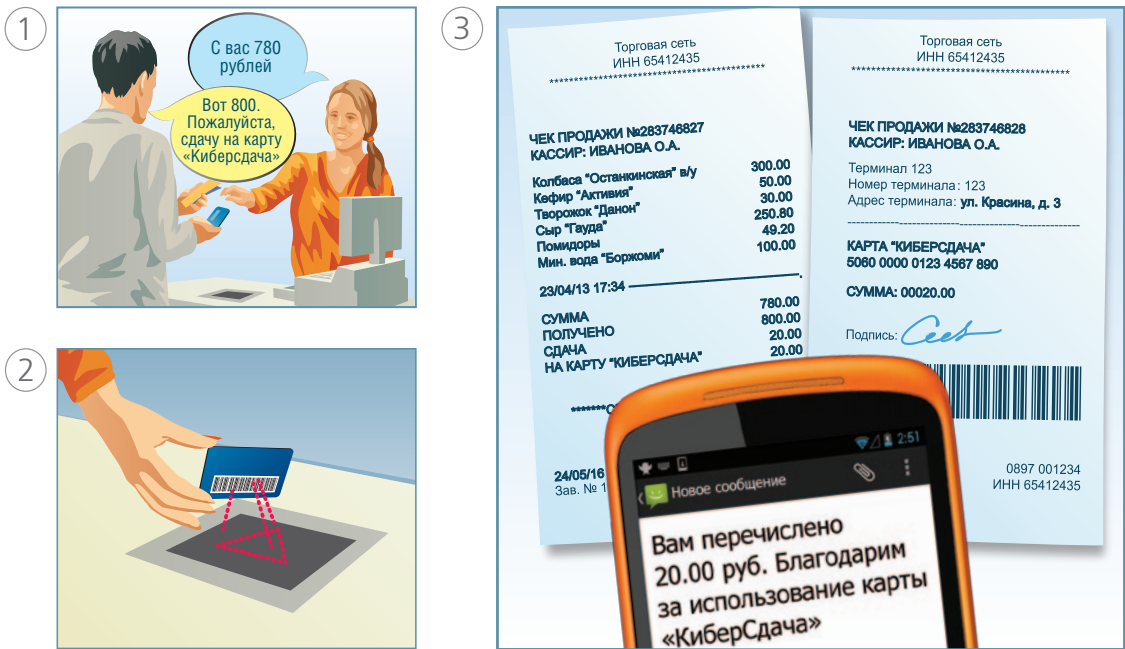
Для операций ниже минимального порога платежа со стороны провайдера клиенту автоматически создается «Платёжная книжка» Plat.ru, и сумма сдачи начисляется на неё.

КАРТА «КИБЕРСДАЧА»

Карта «КиберСдача» — пластиковая карта, совпадающая по размерам со стандартными картами. На карту нанесены 19-значный номер карты и штрих-код.



ОБЩАЯ СХЕМА ЗАЧИСЛЕНИЯ



Рассмотрим часто встречающуюся ситуацию: в самый неожиданный момент мобильный телефон блокируется, потому что заканчиваются деньги. Человек срочно ищет ближайшую точку приёма платежей, чтобы быстро и удобно пополнить счёт.

Он заходит в ближайший магазин известной ритейловой сети и просит кассира пополнить счёт. В ответ кассир предлагает совершить покупку, а сумму сдачи перечислить на счёт сотового оператора. Человек соглашается, так как понимает, что одновременно и пополняет счёт, и приобретает нужный товар. В итоге увеличивается оборот магазина и растет лояльность покупателей к ритейловой сети.

Количество товаров импульсного спроса в сетях минимаркетов может составлять до 50% оборота, в супер- и гипермаркетах — до 20%.

ПРЕИМУЩЕСТВА ОТКАЗА ОТ ИСПОЛЬЗОВАНИЯ МЕЛОЧИ (МОНЕТ И МЕЛКОЙ КУПЮРЫ) ПРИ СДАЧЕ

Для плательщиков

- Экономия времени в очереди на кассах.
- Экономия времени на пополнении личного счёта у провайдеров различных услуг, так как является сопутствующей операцией.
- Освобождение от необходимости пользоваться монетами, которые неудобно хранить в больших количествах в карманах или в кошельке.
- Позволяет потратить деньги на себя, а не превращать их в «чаевые» кассиру, оставляя ему небольшую сумму сдачи.
- Снижает риски, связанные с использованием негигиеничных в употреблении металлических и бумажных денег.

Для кассиров торговых сетей

- Экономия рабочего времени, затрачиваемого на размен и пересчёт мелких денег.
- Отсутствие необходимости постоянно контролировать наличие мелочи для размена в кассе и привлекать старшего менеджера для размена крупных купюр.
- Отсутствие необходимости просить покупателей готовить мелкие деньги или оплачивать покупки точными суммами без сдачи.
- Рост эффективности и комфорта работы, увеличение скорости обслуживания покупателей, сокращение очередей в кассы.

Для предприятий розничной торговли

- Увеличение товарооборота до 35% в течение года от момента внедрения услуги.
- Уменьшение числа ошибок, связанных с некорректным вводом платёжных реквизитов.
- Ускорение обслуживания покупателя на кассе (ролик «КиберСдача – высокая скорость платежа»: <http://youtube/8PXcbqL5Zt0>).
- Отсутствие необходимости в заказе монет и мелких купюр.
- Уменьшение задержек при размене наличности, в том числе и у других кассиров.
- Уменьшение случаев отказа от покупок из-за отсутствия сдачи и снижение негативного настроения покупателей в очередях.
- Увеличение выручки и экономия на заработной плате кассиров.
- Создание психологического комфорта в работе кассиров и увеличение их КПД.
- Привлечение в торговый зал покупателей, совершающих импульсные покупки.
- Проведение маркетинговых акций в виде бонусов на карты «КиберСдача» в конце года (квартала) в целях мотивации клиентов и увеличения их лояльности.

ПРЕИМУЩЕСТВА УНИКАЛЬНОГО ФИНАНСОВОГО СЕРВИСА «КИБЕРСДАЧА»

Для плательщиков

- Быстрое зачисление денег.
- Исключение ошибок ручного ввода номеров телефонов и других идентификаторов платежей.
- Сохранение приватности персональных данных, так как нет необходимости называть номер телефона вслух.
- Нет необходимости передавать банковскую карту в чужие руки. Наоборот, можно всем раздавать карту, привязанную к своему номеру: «пусть кладут свою сдачу мне на счёт».
- Возможность положить на счёт не только сдачу, но и большую сумму (до 15 тысяч рублей).
- SMS-подтверждение о зачислении суммы сдачи.
- Возможность зачислить сумму сдачи на банковскую карту, в том числе несколько раз, а денежные средства затем снять в банкомате.

Для ритейловых сетей

- Исключение ошибок ручного ввода номеров телефонов и других идентификаторов платежей.
- Ускорение обслуживания покупателей на кассе (кассиры не тратят время на выдачу сдачи).
- Нет необходимости заказывать монеты и мелкие купюры в банке.
- Экономия затрат на инкассацию, так как инкассация монет и мелких купюр тарифицируется банками по повышенной ставке.
- Простое подключение: только один шлюз «КиберСдача» вместо группы шлюзов (Visa Money Transfer, MasterCard Money Send, шлюзы банков, шлюзы провайдеров).
- Использование информации о покупателе (номер карты «КиберСдача»), полученной при оплате, в рекламных и маркетинговых целях: составление «портрета» покупателя, адресная SMS-рассылка через «КиберПлат» (CyberPlat®) о скидках и расширении товарного ассортимента и многое другое.
- Расширение возможностей собственных программ лояльности путём начисления бонусов и проведения мотивирующих акций.
- Рост продаж товаров импульсного спроса благодаря удобству оплаты мобильной связи на кассах.
- Удобный и быстрый приём «тяжелых» платежей (оплата штрафов ГИБДД, пополнение карт и банковских счетов, погашение кредитов, оплата ЖКХ и др.) с помощью карты «КиберСдача» привлекает дополнительную клиентуру со средней и высокой покупательской способностью в ритейловые сети.

ОЦЕНКА ЭФФЕКТИВНОСТИ

Сравнительный анализ продуктового ритейла для магазинов среднего и малого форматов показал следующую статистику

	Средний магазин	Малый магазин
Торговая площадь, кв. м	До 1 500	До 200
Среднее количество касс	4	2
Среднее количество чеков в день на кассу, шт.	460	460
Увеличение посещаемости супермаркетов от внедрения проекта «КиберСдача», %	20	30
Размер среднего чека, руб.	359	233
Средний размер сдачи, руб.	270	263

Показатели операционной эффективности*

	Прямые затраты (себестоимость товаров), %	Непрямые затраты (зарплата персонала, аренда и т.д.), %
Группа X5	74	21
Группа МАГНИТ	71	21
Группа ДИКСИ	66	25

* <http://www.dixygroup.ru/~media/Files/D/Dixy/financial-results/archive2014/RUS/FY2014RUS.pdf>
http://www.x5.ru/ru/investors/financial_reports
<http://ir.magnit.com/financial-reports-rus>

Пример малой продовольственной розницы*

	Оценка до внедрения «КиберСдачи»	Оценка после внедрения «КиберСдачи»
Среднее количество касс	2	3
Среднее количество чеков в месяц для магазина из 2 касс	27 600	37 260
Размер среднего чека, руб.	233	233
Оборот магазина в год, млн руб.	77,2	104,2
Средние прямые затраты (стоимость товаров), % от выручки	74	74
Средние прямые затраты (стоимость товаров), млн руб.	57,1	77,1
Средние непрямые затраты (зарплата, аренда и т.д.), % от выручки	17	13
Средние непрямые затраты (зарплата, аренда и т.д.), млн руб.	13,1	13,8
Средняя рентабельность, млн руб.	6,9	13,3
Средняя рентабельность, %	9	13

* Данные оценены по финансовой отчетности ДИКСИ, Магнита, X5.

Прирост рентабельности составляет 6,4 млн рублей на один магазин в год.

- Выручка увеличивается на 35%.
- Зарплаты вырастают на 5%, а арендные платежи остаются теми же самыми. Данный рост рентабельности может быть достигнут за 1–2 месяца после насыщения базы постоянных покупателей картами «КиберСдача».

Пример супермаркета среднего формата*

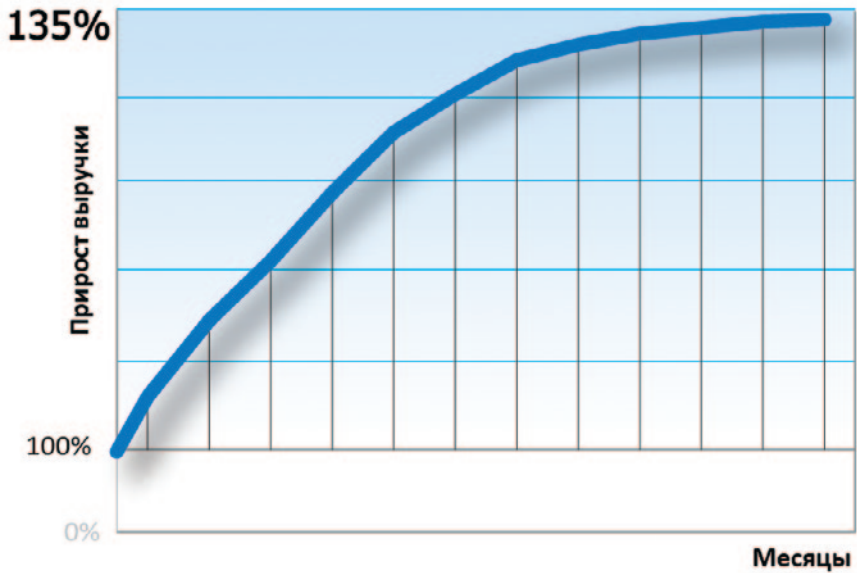
	Оценка до внедрения «КиберСдачи»	Оценка после внедрения «КиберСдачи»
Среднее количество касс	4	3
Среднее количество чеков в месяц для магазина из 2 касс	55 200	37 260
Размер среднего чека, руб.	359	233
Оборот магазина в год, млн руб.	237,8	104,2
Средние прямые затраты (стоимость товаров), % от выручки	74	74
Средние прямые затраты (стоимость товаров), млн руб.	176,0	77,1
Средние не прямые затраты (зарплата, аренда и т.д.), % от выручки	19	13
Средние не прямые затраты (зарплата, аренда и т.д.), млн руб.	45,2	13,8
Средняя рентабельность, млн руб.	16,6	13,3
Средняя рентабельность, %	7	13

* Данные оценены по финансовой отчетности ДИКСИ, Магнита, Х5.

Прирост рентабельности составляет 13,2 млн рублей на один магазин в год.

- Выручка увеличивается на 35%.
- Зарплаты вырастают на 5%, а арендные платежи остаются теми же самыми. Данный рост рентабельности может быть достигнут за 2–3 месяца после насыщения базы постоянных покупателей картами «КиберСдачи».

ГРАФИК ОЖИДАЕМОГО ПРИРОСТА ВЫРУЧКИ ИЗ-ЗА УВЕЛИЧЕНИЯ ФУТ-ТРАФИКА



Сравнение эффективности внедрения проекта «КиберСдача» в малой и средней рознице

Проект «КиберСдача» благоприятно сказывается на увеличении оборота торговой точки в магазинах малой и средней розницы, подключённых к сервису. Рост рентабельности может быть достигнут в течение 3–6 месяцев.

Таким образом, внедрение «КиберСдачи» для малых магазинов более привлекательно, чем для более крупных форматов.

	Показатели малой продовольственной сети после внедрения «КиберСдачи»	Показатели супермаркета среднего формата после внедрения «КиберСдачи»
На сколько увеличится средняя рентабельность, %	На 4	На 3
На сколько увеличится выручка с квадратного метра, %	На 26	На 20

РОСТ ОБОРОТА ВЫСОКОМАРЖИНАЛЬНЫХ ТОВАРОВ

С ростом фут-трафика в результате внедрения проекта «КиберСдача» в торговой точке увеличивается оборот высокомаржинальных товаров. Клиент приходит оплачивать услуги с помощью карты «КиберСдача» и совершает покупки высокодоходных товаров импульсного спроса, расположенных в прикассовых зонах.

В электронном ритейле происходит рост продаж аксессуаров: чехлов к мобильным телефонам, брелоков, карт памяти, батареек и т.п.

В продуктовом ритейле растет реализация пива, сигарет, алкоголя, минеральной воды, шоколада, кондитерских изделий, жевательной резинки, а также увеличиваются продажи непродовольственных высокомаржинальных товаров.

ВЛИЯНИЕ СЕРВИСА НА ТЕРМИНАЛЫ, УСТАНОВЛЕННЫЕ В ТОРГОВЫХ СЕТЯХ

В торговых сетях, как правило, уже стоят платёжные терминалы, которые приносят сетям дополнительный доход в виде арендной платы. Запуск проекта «КиберСдача» окажет положительное влияние на доходность установленных терминалов в силу ряда причин.

1. Большинство мелких платежей на сумму от 10 до 100 рублей будут приниматься на кассах, а не через терминал. В итоге:
 - значительно снизится нагрузка на терминал, так как мелкие платежи составляют до 70% транзакций, но лишь 5% от общей суммы;
 - резко уменьшится количество претензий клиентов, так как 90% проблем связано с зачислением мелких платежей. Это приведет к снижению нагрузки на службу поддержки клиентов терминальной сети;
 - уменьшатся затраты на инкассацию мелких купюр из терминалов, так как практически все они будут приниматься на кассах.



2. Терминалы крайне редко оборудованы сканером штрих-кодов, поэтому приём платежей в пользу ГИБДД, поставщиков услуг ЖКХ и налоговых органов на кассе только увеличит число клиентов торговой сети. Соответственно, увеличится клиентский поток крупных платежей через терминалы. Даже если в терминале есть сканер штрих-кодов, эти шлюзы для владельцев терминалов обычно являются ассортиментной услугой, а не источником основных доходов.
3. Основной доход терминального бизнеса — погашение кредитов в сумме от 2000 до 5000 рублей — останется, поскольку:
 - очень сложно представить себе человека на кассе, совершающего мелкую покупку (например, пива или чипсов) и расплачивающегося за нее пятитысячной купюрой;
 - эти платежи почти всегда осуществляются с внешней дополнительной комиссией с плательщика;
 - взимание комиссии за платежи сдачи на кассе вызовет негатив у покупателей, поэтому, скорее всего, торговые сети не будут реализовывать погашение кредитов на кассе.
4. На терминалах, имеющих сканер штрих-кодов, можно проводить активацию карт «КиберСдача», что будет приносить стабильный хороший доход владельцу терминала. Сумма комиссий за активацию будет определяться торговой сетью.
5. Опыт показал, что карта «КиберСдача» оказалась очень удобной при оплате в терминале. Клиенты, активировавшие карту на кассе, стали значительно чаще платить в терминалах.



ЗАЧИСЛЕНИЕ СДАЧИ

Зачисление на интеллектуальных кассах

- Кассир сканирует карту стационарным или ручным сканером или вводит номер карты на клавиатуре.
- При использовании интеллектуального кассового аппарата со считывателем штрих-кодов происходит сканирование штрих-кода с карты «КиберСдача».

При этом в обоих случаях сумма сдачи уже находится в памяти кассового аппарата.

Зачисление в мелких торговых точках

При отсутствии на торговой точке кассового аппарата с широким функционалом можно использовать недорогие модели Android-смартфонов.

На смартфон устанавливается приложение Cyberplat Mobile, которое позволяет считывать штрих-код с карты «КиберСдача». При этом сумма сдачи вводится продавцом вручную или передаётся с присоединённого компьютера с установленным ПО «Кабинет дилера».

Платёж в терминалах самообслуживания

- При наличии считывателя штрих-кодов в терминале происходит сканирование штрих-кода с карты «КиберСдача».
- ПО платёжного терминала сразу отображает на экране провайдера «КиберСдача» и номер карты (шаблона).

Сумма оплаты указывается после внесения клиентом денег в купюроприёмник и нажатия кнопки «Далее».



КАК АКТИВИРОВАТЬ КАРТУ

Активация на сайтах www.киберсдача.рф и www.plat.ru

1. Клиент заходит на страницу активации карт на www.киберсдача.рф или www.plat.ru, вводит номер имеющейся карты, выбирает получателя платежа, указывает номер телефона и для защиты от мошенничества вводит отображенный код CAPTCHA.
2. Сервис сайта обращается к базе данных «КиберПлат» (CyberPlat®) и проверяет, активирована ли карта. В случае если карта ещё не активирована, клиенту предлагается выбрать провайдера и ввести требуемые данные: номер лицевого счёта провайдера, номер мобильного телефона и другую информацию.
3. Клиент вводит запрошенные данные.
Примеры ввода данных:
МТС, 985-222-33-22;
VISA, 1234 5678 9012 3456;
Пополнение счетов в Альфа-банке, р/с 40817810123456789012, 985-111-22-33.
4. Получив данные, система «КиберПлат» (CyberPlat®) присваивает данному номеру карты введённый шаблон и направляет клиенту SMS-подтверждение об активации карты.

Активация с помощью системы предварительно записанных голосовых сообщений (IVR)

1. Клиент звонит по многоканальному номеру +7(499)68-111-58.
2. Приятный голос сообщает: «Здравствуйте, Вы позвонили в службу активации карт “КиберСдача”. Введите, пожалуйста, номер карты».
3. Клиент вводит 19-значный номер имеющейся карты.
4. Сервис проверяет, активирована ли карта. Если карта уже активирована, получает отказ от БД «КиберПлат» (CyberPlat®).
5. Клиент слышит: «К сожалению, эта карта уже активирована. Введите номер другой карты», далее п. 3.
6. Если карта ещё не активирована, система определяет номер телефона, с которого совершается звонок, и клиент слышит: «Ваш телефонный номер “NNNNNNNNNN” Нажмите “*” для привязки этого номера к карте “КиберСдача”. Если необходимо привязать другой мобильный номер, введите нужный 10-значный телефонный номер, включая префикс, и подтвердите правильность нажатием “*”».
7. Клиент вводит нужный номер телефона, например, «985 123 45 67».
8. Клиент слышит: «Операция успешно завершена. К Вашей карте с номером 000 0000 0000 0000 1234 привязан номер телефона 985 123 45 67. Повторяю, операция успешно завершена. К Вашей карте с номером 000 0000 0000 0000 1234 привязан номер телефона 985 123 45 67» (3 повтора).
9. В случае ошибки при введении телефонного номера клиент слышит: «Внимание: ошибка! Указан некорректный номер телефона. Пожалуйста, введите правильный 10-значный номер телефона и нажмете “*”».

Активация на платёжных терминалах самообслуживания

Клиент может провести активацию карты только на терминалах, оборудованных сканером штрих-кодов.

1. После выполнения обычной операции «приём платежа» клиент выбирает в ПО терминала функцию «Присвоить шаблону платежа номер карты "КиберСдача"».
2. Клиент сканирует номер неактивированной карты в сканере штрих-кодов.
3. ПО терминала обращается к БД «КиберПлат» (CyberPlat®) по шлюзу «КиберСдача-эмиссия (введение шаблона)» и проверяет, активирована ли карта. Если карта ещё не активирована, передаёт код провайдера, номер лицевого счёта у провайдера, номер мобильного телефона и иную информацию.
4. «КиберПлат» (CyberPlat®) присваивает данному номеру карты введенный шаблон и подтверждает в ПО терминала.

Хранение персональных данных — наименование провайдера, номер лицевого счёта у провайдера, номер мобильного телефона и их соответствие номеру шаблона — запрещено правилами платёжного сервиса «КиберСдача».

Активация на кассовых аппаратах

1. После выполнения обычной операции «приём платежа» кассир выбирает в ПО кассы (или ПО «Кабинет дилера») функцию «Присвоить шаблону номер карты "КиберСдача"».
2. Клиент сканирует номер неактивированной карты стационарным или ручным сканером или вводит на клавиатуре номер карты.
3. ПО кассы обращается к БД «КиберПлат» (CyberPlat®) и, если карта ещё не активирована, передаёт код провайдера, номер лицевого счёта у провайдера, номер мобильного телефона и иную информацию.
4. «КиберПлат» (CyberPlat®) присваивает данному номеру карты введенный шаблон и подтверждает операцию в ПО кассы или ПО «Кабинет дилера».
5. Кассир отдает карту клиенту со словами: «В следующий раз приходите с этой картой, будет быстрее. Возьмите с собой ещё пару неактивированных карт для членов семьи, активируете дома на сайтах www.киберсдача.рф и www.plat.ru.

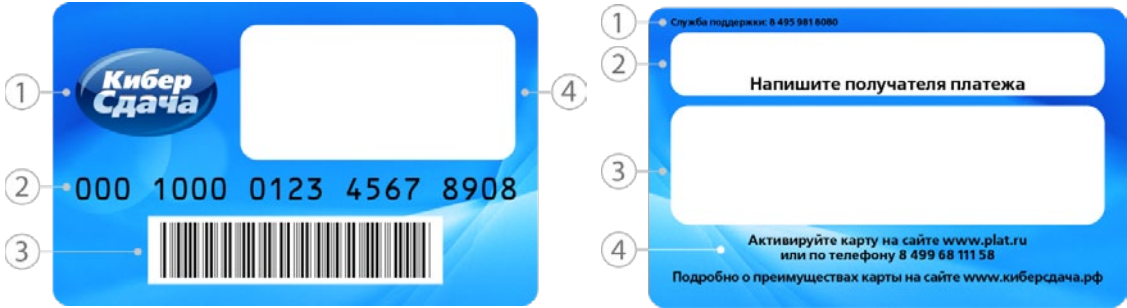
Хранение персональных данных — наименование провайдера, номер лицевого счёта у провайдера и их соответствие номеру шаблона — запрещено правилами платёжного сервиса «КиберСдача».

Преимущества для «активаторов» карт на кассах и терминалах

Ритейловые сети и владельцы терминалов, использующие этот современный сервис, в сравнении с остальными участниками рынка получают серьёзные конкурентные преимущества, которые заключаются:

- в ускорении операций по приёму платежей;
- повышении лояльности клиентов благодаря внедрению нового удобного сервиса;
- получении дополнительного дохода от эмиссии активированных карт с рекламой рекламодателя;
- получении дохода от комиссии за платёж на любой другой точке. В первый год это фиксированная величина, которая определяется в зависимости от оборота по активированной карте.

КАК ВЫГЛЯДИТ КАРТА «КИБЕРСДАЧА»



Внешнее оформление и дизайн

Карта «КиберСдача» соответствует размерам стандартной банковской карты. На лицевой стороне карты есть следующие отличительные особенности:

1. Логотип «КиберСдача».
2. Номер карты: 19 цифр, первые три из которых всегда ноль.
3. Штрих-код.
4. Поле для рекламы эмитента.

На оборотной стороне карты имеются следующие отличительные особенности:

1. Телефоны службы поддержки эмитента.
2. Бумажная полоса для нанесения получателя платежа вручную.
3. Место для рекламы.
4. Подробная инструкция по активации.

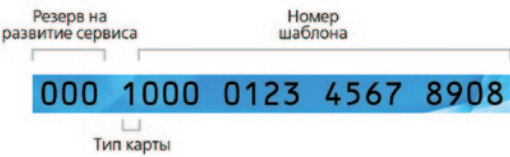
Также на оборотной стороне карты может быть наклеен стикер со штрих-кодом, который при необходимости можно переклеить на обратную сторону мобильного телефона.

Первые три цифры в номере карты всегда являются 0. Это особенность нумерации карт установлена для резервирования базы карточных номеров на развитие сервиса.

Номер шаблона, присвоенный в системе «КиберПлат» (CyberPlat®) для данной карты, содержит 16 цифр, которые отражают тип карты и шаблон, соответствующий набору данных в базе данных «КиберПлат» (CyberPlat®):

1. Провайдер услуги. Например, МТС.
2. Лицевой (или банковский счёт) в учётной системе провайдера. Например, 79851112233.
3. Иная информация.

Формат номеров и номер шаблона



Тип карты
1 – КиберСдача
2 – КиберСдача хэви
3 – Киберплатеж

В типе карты цифра 1 означает, что это карта «КиберСдача», цифра 2 — карта «КиберСдача хэви», цифра 3 — карта «Киберплатеж».

ВИРТУАЛЬНАЯ КАРТА «КИБЕРСДАЧА»

Карта «КиберСдача» может быть эмитирована в электронном, виртуальном виде в интернете, сохранена в качестве файла и использоваться при считывании с экрана телефона.

- Клиент заходит на сайт www.plat.ru и в разделе «Активируй карту «КиберСдача» указывает реквизиты поставщика услуги, номер мобильного телефона, а для защиты от мошенничества вводит отображенный код САРТСНА.
- Система генерирует новый номер карты, отражает на экране штрих-код и отправляет на указанный номер мобильного телефона SMS со ссылкой на загрузку этого кода.



ЭМИССИЯ КАРТ «КИБЕРСДАЧА»

Массовая эмиссия неактивированных карт

Карты печатаются массовым тиражом эмитентом, заключившим договор о реализации сервиса «КиберСдача», в рамках выделенного системой «КиберПлат» (CyberPlat®) массива номеров карт.

Для распространения карт используются технологии максимального охвата целевой аудитории, включая:

- массовую почтовую рассылку;
- раздачу на кассах гипер- и супермаркетов, торгово-развлекательных центров и иных мест с высоким покупательским трафиком;
- размещение в прикассовых зонах, а также возле платёжных терминалов.

Массовая эмиссия предактивированных карт эмитентом-провайдером

Наибольшую заинтересованность в массовой эмиссии карт проявляют операторы сотовой связи, банки, особенно с развитой розничной сетью, а также провайдеры, услугами которых пользуется практически каждый житель страны, например энергосбытовые компании.

1. Эмитент-провайдер обращается к «КиберПлат» (CyberPlat®) и передаёт диапазон номеров телефонов или лицевого счета.
2. «КиберПлат» (CyberPlat®) присваивает полученным номерам ещё не занятые номера карт и сообщает их эмитенту.
3. Эмитент-провайдер в соответствии с полученными от «КиберПлат» (CyberPlat®) данными самостоятельно печатает карты в типографии.
4. Эмитент-провайдер распространяет карты с помощью массовой рассылки по адресам своих абонентов, а также раздаёт в своих и партнёрских офисах обслуживания.

КАРТА «КИБЕРСДАЧА», ПРЕДАКТИВИРОВАННАЯ ЭМИТЕНТОМ-ПРОВАЙДЕРОМ

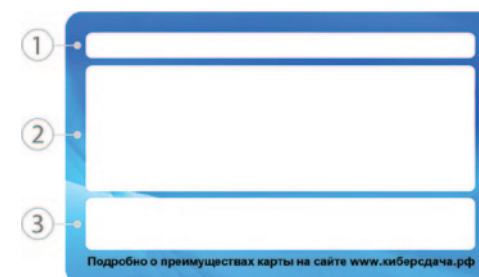
Лицевая сторона карты:

1. Логотип «КиберСдача».
2. Номер карты.
3. Название карты (присутствует только на предактивированных картах).
4. Штрих-код.
5. Поле для рекламы эмитента.



Оборотная сторона карты:

1. Телефоны службы поддержки эмитента.
2. Место для рекламы.
3. Контактная информация эмитента.



Пример эмитента «КиберПлат»

Служба
поддержки

Служба поддержки:
+7 (495) 981-80-80

Контактная
информация

Подробнее о преимуществах карты на сайте www.киберсдача.рф
Карта является собственностью ООО «КИБЕРПЛАТ».
123610, Москва, Краснопресненская наб., 12, подъезд 7, 12 этаж.

ПРИВЯЗКА КАРТЫ «КИБЕРСДАЧА» К ПРОГРАММЕ ЛОЯЛЬНОСТИ ТОРГОВОЙ СЕТИ

Карта «КиберСдача» может быть совмещена с картой лояльности торговой сети либо привязана к ней. При этом торговая сеть сама определяет соответствие номеров карт «КиберСдача» номерам карт лояльности и самостоятельно выполняет действия по начислению баллов и выдаче торговых бонусов.

Проектное взаимодействие может проходить по следующим сценариям.

1. «КиберПлат» (CyberPlat®) предоставляет торговой сети диапазон номеров карт (штрих-кодов). Торговая сеть эмитирует наполовину активированные карты «КиберСдача» со своим логотипом, в которых карта лояльности уже привязана, а платёжные реквизиты ещё нет. Торговая сеть раздаёт карты клиентам, и клиенты самостоятельно привязывают карты на нужные в каждом конкретном случае платёжные реквизиты: например, номер мобильного телефона или лицевой счёт в управляющей компании, обслуживающей его квартиру.
2. Торговая сеть может привязать уже имеющуюся у клиента карту «КиберСдача» к новой карте лояльности ритейлера. В этом случае у клиента исчезает необходимость носить с собой карту лояльности торговой сети, так как в качестве идентификатора при получении бонусов от сети он будет использовать карту «КиберСдача».

КАРТА «КИБЕРСДАЧА ХЭВИ»



Отличие карты «КиберСдача хэви»

На карту «КиберСдача» гарантированно можно перевести сумму сдачи, начиная от одной копейки и выше. Это очень удобно, когда после оплаты покупки остаётся небольшая сдача, например 1 рубль 20 копеек, и её можно перевести на счёт мобильного телефона.

При этом не каждый клиент захочет переводить на мобильный телефон существенную сумму, например 800 рублей. Если необходимо погасить кредит или пополнять банковскую карту, клиенту удобно перечислить крупную сумму сдачи именно туда, но в ряде случаев банки (и некоторые провайдеры) взимают комиссию за зачисление денег на счёт.

Чтобы отличить карты, по которым суммы могут зачисляться без комиссии, от карт, по которым невозможно зачисление без комиссии, специально введена карта «КиберСдача хэви».

С помощью карты «КиберСдача хэви» можно переводить денежные средства провайдерам услуг, приём платежей в пользу которых осуществляется с обязательным взиманием дополнительной комиссии.

Карту «КиберСдача хэви» рекомендуется использовать для пополнения карт Мир, Visa, MasterCard, внесения денежных средств на банковские счета, а также для совершения других регулярных платежей.

Внешнее оформление и дизайн

Карта «КиберСдача хэви» визуально отличается только наличием в названии знака «хэви».

Функционально это означает, что с её помощью приём платежей осуществляется с обязательным взиманием дополнительной комиссии с плательщика

Лицевая сторона карты:

1. Логотип «КиберСдача хэви».
2. Номер карты из 19 цифр, первые четыре цифры: 000 2.
3. Штрих-код.
4. Поле для рекламы эмитента.

Оборотная сторона выглядит так же, как у обычной карты «КиберСдача».

ПРЕДЛОЖЕНИЯ ДЛЯ РЕКЛАМОДАТЕЛЕЙ

Пример быстрой «раскрутки» торговой сети, принимающей карты «КиберСдача» в пользу сотового оператора

Партнёрство торговой сети и оператора мобильной связи в реализации сервиса «КиберСдача» носит взаимовыгодный характер. Ритейлер, принимающий карты «КиберСдача» в пользу сотового оператора, получает существенные преимущества для динамичного роста покупательского трафика и, следовательно, увеличения оборота торговых точек. Мобильный оператор, помимо стабильного роста объёма платежей имеет возможность без особых затрат с максимальной точностью таргетировать аудиторию для развития абонентской базы: например, выбирать определённый населённый пункт или даже его конкретный район.

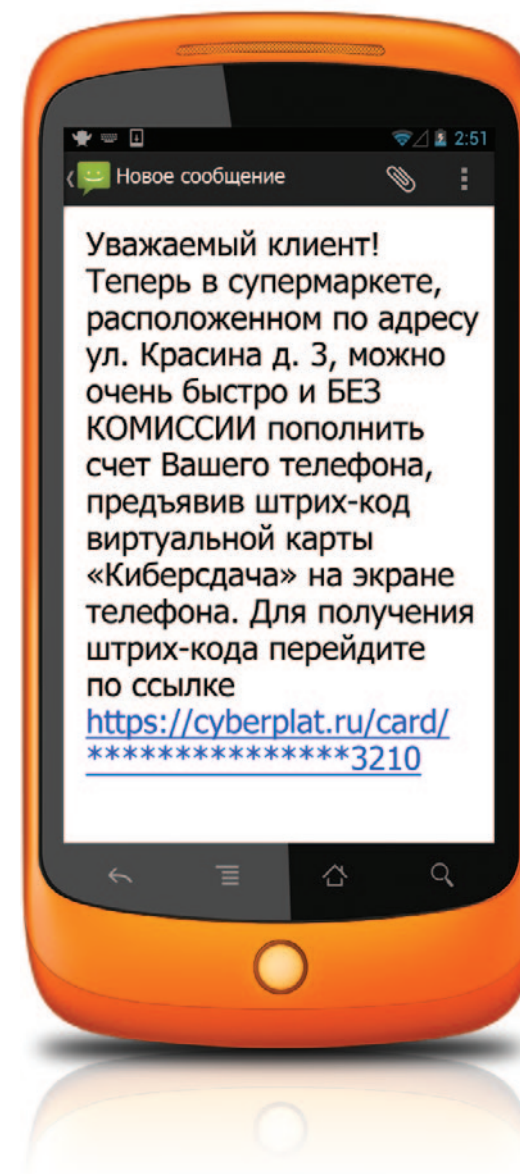
Алгоритм взаимодействия следующий.

1. Заключается предварительное соглашение между розничной торговой сетью (супер- или гипермаркет) и сотовым оператором.
2. Достаточно крупная торговая точка подключается к приёму карт «КиберСдача».
3. Сотовый оператор рассылает своим клиентам, проживающим в радиусе только одной соты, сообщение примерного содержания: «Уважаемый клиент! Теперь в супермаркете, расположенном по адресу (указывается адрес), можно очень быстро пополнить счёт вашего телефона, предъявив штрих-код виртуальной карты "КиберСдача" на экране телефона. Для получения штрих-кода перейдите по ссылке».
4. Заинтересовавшийся клиент приходит в супермаркет и пробует услугу.
5. Кассир, предварительно прошедший обучение, выдаёт покупателю неактивированную карту с напечатанной на ней рекламой торговой сети со словами: «С телефона считывает не всегда хорошо. Пожалуйста, активируйте себе карту на пластике». Сразу за этим предлагает плательщику взять ещё несколько неактивированных карт для себя или своих близких и друзей, а также рекламную листовку с подробным описанием преимуществ сервиса.

Пример быстрой «раскрутки» сети приёма платежей, принимающей карты «КиберСдача»

Сеть пунктов приёма платежей обладает большим потенциалом роста доходности с точки зрения реализации сервиса «КиберСдача» на кассах. Для быстрой и эффективной раскрутки необходимо использовать имеющуюся клиентскую базу для целевой SMS-рассылки* с приглашением воспользоваться новым современным и удобным сервисом.

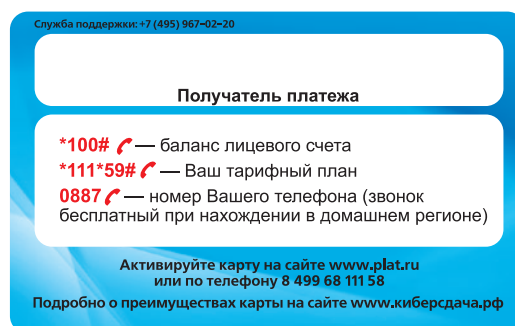
Клиент получает сообщение со ссылкой на виртуальную карту «КиберСдача», уже привязанную к номеру его мобильного телефона, скачивает штрих-код из сообщения и при следующем платеже на кассе использует экран телефона для совершения платежа.



* SMS-рассылка осуществляется только с согласия абонента.

ПРЕИМУЩЕСТВА ДЛЯ ПРОВАЙДЕРОВ-ЭМИТЕНТОВ*, ВЫПУСКАЮЩИХ КАРТЫ «КИБЕРСДАЧА» СО СВОИМ ЛОГОТИПОМ

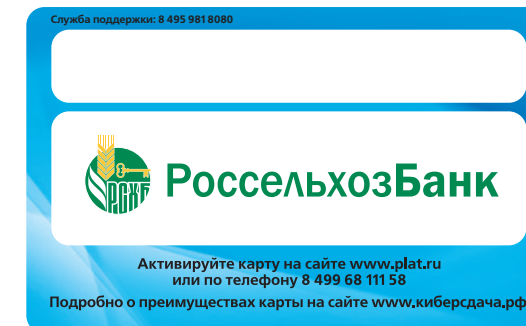
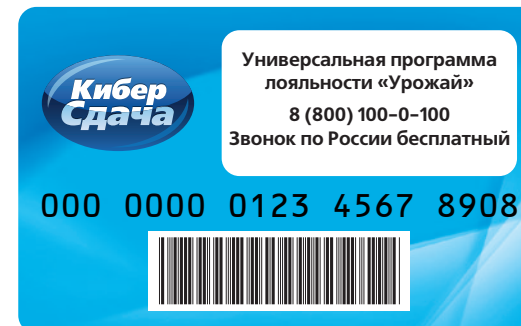
1. По экспертным оценкам, в масштабах страны потенциал роста суммы поступлений средств на лицевые счета абонентов на сумму сдачи составляет \$72,5 миллиардов. Он складывается из \$60 миллиардов, которые можно получить в продовольственном ритейле, и \$12,5 миллиардов — в непродовольственной розничной торговле. Эта величина существенно выше всей выручки сотовой связи России.
2. Существенное облегчение конкурентной борьбы за клиентов при минимуме затрат, так как «КиберПлат» (CyberPlat®) представляет платёжную инфраструктуру и выступает катализатором процесса.
3. Повышение лояльности абонентов благодаря новому современному и удобному сервису.
4. Увеличение ARPU — одного из ключевых показателей эффективности бизнеса.
5. Снижение периода молчания абонента из-за блокировки номера в связи с отсутствием денег на счёте, а также существенное уменьшение вероятности возникновения такой ситуации.
6. Увеличение объёма информации о клиенте для проведения более точных маркетинговых мероприятий.



* Названия организаций приведены в качестве примера.

ПРЕИМУЩЕСТВА ДЛЯ БАНКОВ-ЭМИТЕНТОВ*, ВЫПУСКАЮЩИХ КАРТЫ «КИБЕРСДАЧА» СО СВОИМ ЛОГОТИПОМ

1. Увеличение поступлений на расчётные счета физических лиц, являющихся клиентами банков, на сумму сдачи.
2. Улучшение «погашаемости» кредитов и повышение платёжной дисциплины клиентов в целом.
3. Отслеживание динамики изменения лояльности клиента к погашению кредита.
4. Увеличение объёма информации о клиенте для проведения более точных маркетинговых мероприятий.
5. Отсутствие конкурентной борьбы за клиента со стороны разработчика сервиса. Наоборот, «КиберПлат» (CyberPlat®) представляет банкам платёжную инфраструктуру и является катализатором процесса. Повышение лояльности клиентов банка благодаря новому современному и удобному сервису.
6. Исключение риска скимминга, поскольку нет необходимости использовать банковские карты.
7. Очень простое начало работ: сумма сдачи поступает на банковские счета посредством уже имеющихся в системе «КиберПлат» (CyberPlat®) платёжных шлюзов НСПК «Мир», Visa Money Transfer и MasterCard Money Send. В дальнейшем при необходимости можно разработать прямой шлюз между банком-эмитентом и «КиберПлат» (CyberPlat®), чтобы дополнительно снизить затраты на пополнение банковских счетов.



* Названия организаций приведены в качестве примера.

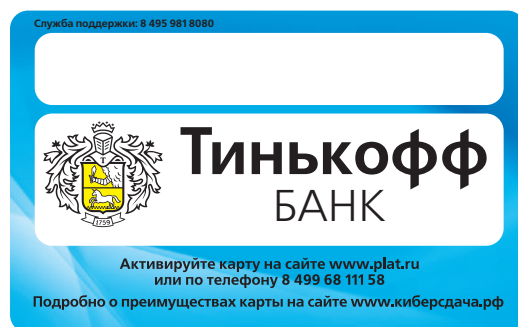
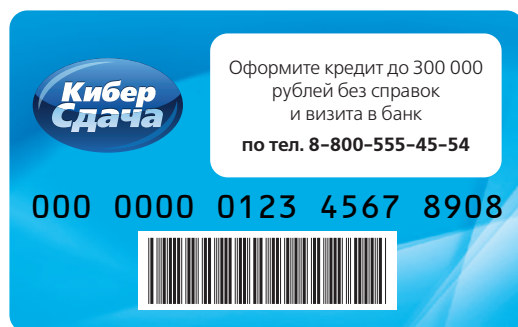
ПРЕИМУЩЕСТВА ДЛЯ ЭМИТЕНТОВ-РЕКЛАМОДАТЕЛЕЙ*, ВЫПУСКАЮЩИХ КАРТЫ «КИБЕРСДАЧА» СО СВОИМ ЛОГОТИПОМ

Тинькофф банк, проведя эмиссию брендированных карт «КиберСдача-Тинькофф», сможет охватить все население Москвы, затратив не более \$10 миллионов. При этом количество использований карты одним потребителем составит от 10 до 40 раз в месяц.

Для распространения карт Тинькофф банк использует технологии максимального охвата целевой аудитории:

- раздача карт кассирам супермаркетов, размещение карт в прикассовых зонах, а также в местах проведения платежей (салоны связи, пункты приёма платежей за коммунальные услуги и т.д.);
- прямая онлайн- и офлайн-рассылка.

По нашим оценкам затраты на маркетинговые мероприятия составят приблизительно \$1 на потенциального пользователя карты, а расходы на производство пластика не превысят \$0,01 на карту.



* Названия организаций приведены в качестве примера.

МАССОВАЯ ЭМИССИЯ КАРТ*

МАССОВАЯ ЭМИССИЯ БАНКОМ

Агрессивный банк, например Тинькофф банк, выпускает карты с логотипом банка и рекламой финансовых услуг массовым тиражом и бесплатно раздаёт их клиентам.

Экономическая эффективность сервиса карты «КиберСдача-Тинькофф» определяется лояльностью потенциального клиента. В среднем держатели карт пользуются ими от 10 до 40 раз в месяц и в связи с большой потребностью хранят «под рукой» в кошельке. Проводя платежи, клиент, как правило, информирует окружающих, многие из которых впервые видят карту, о её возможностях, удобстве и функциональности.

ВОЗМОЖНАЯ ЗАЩИТА КОНКУРЕНТОВ

Банку-конкуренту, предлагающему стандартный набор финансовых сервисов, в который не входит карта «КиберСдача», для максимально быстрого ответа в условиях жёсткого дефицита времени приходится использовать технологию «отзеркаливания».

Банк оперативно проводит эмиссию карт и осуществляет массовую рассылку предактивированных карт «КиберСдача» со своим логотипом и рекламой услуг.

Для снижения затрат банк вынужден ориентироваться на контролируемый ритейл. Например, Альфа-банк в первую очередь станет осуществлять массовую раздачу неактивированных карт в торговых сетях X5 Retail Group.

МАССОВАЯ ЭМИССИЯ ПРОВАЙДЕРОМ СВЯЗИ

Агрессивный провайдер связи, например МТС, в салонах бесплатно раздаёт клиентам карты со своим логотипом и рекламой сервисов МТС.

Экономическая эффективность сервиса карты «КиберСдача-МТС» определяется лояльностью потенциального клиента. Держатели этих карт пользуются ими до 40 раз в месяц, поэтому хранят в кошельке вместе с банковскими картами. Проводя платежи, клиенты могут информировать окружающих, многие из которых впервые видят карту, о её возможностях, удобстве и функциональности.

Действия конкурента, например, компании Билайн

Защита: массовая рассылка предактивированных карт «КиберСдача-Билайн» с логотипом Билайна своим клиентам.

Атака: массовая раздача неактивированных карт в дружественном ритейле, например, в сети магазинов «Седьмой континент».

МАССОВАЯ ЭМИССИЯ НЕАКТИВИРОВАННЫХ КАРТ РЕКЛАМОДАТЕЛЕМ

Агрессивный рекламодатель, например компания «Кока-Кола», осуществляет массовую бесплатную раздачу карт с нанесенным логотипом и рекламой напитка.

Экономическая эффективность карты «КиберСдача-Кока-Кола» определяется лояльностью потенциального владельца, которая характеризуется указанными выше параметрами. Несмотря на широкую известность бренда «Кока-Кола», необычный рекламный носитель привлекает внимание окружающих, многие из которых никогда не видели такую карту.

Защита конкурента, например, компании «Пепси-Кола»

Традиционный конкурент «Кока-Колы» для эффективного ответа вынужден также эмитировать карту со своим логотипом и в целях экономии времени и ресурсов массово распространять неактивированные карты в дружественном ритейле, например, в сети ресторанов быстрого питания «Макдональдс».



* Названия организаций приведены в качестве примера.

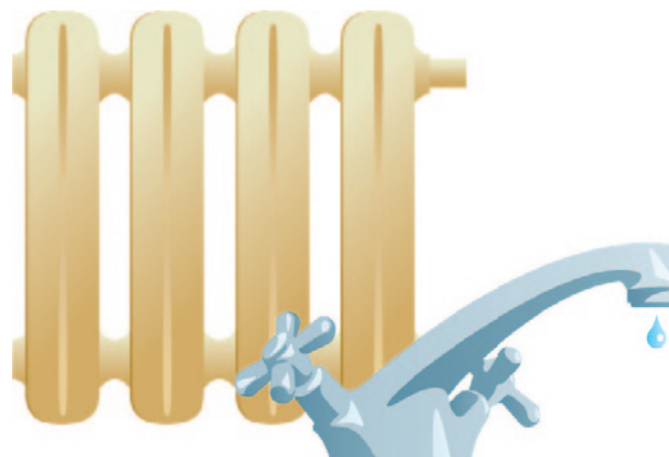
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ДЛЯ РАЗВИТИЯ БИЗНЕСА

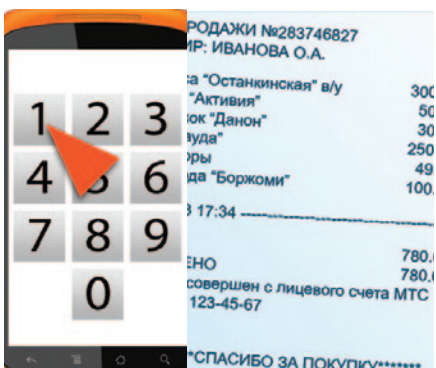
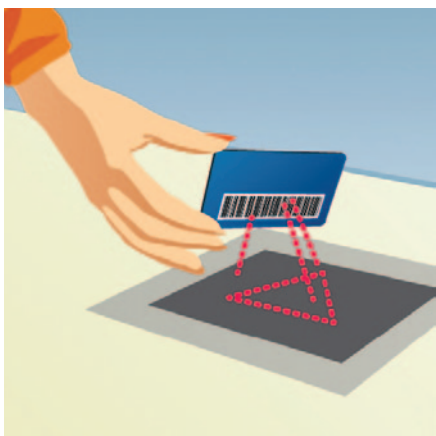
Платёжи по штрих-коду

Благодаря универсальности решения «КиберСдача» позволяет реализовать дополнительные клиентские сервисы исходя из задач, стоящих перед компаниями.

Если ритейлер заинтересован в притоке клиентов со средней и высокой степенью покупательской способности («богатых» покупателей), то на кассах торговой сети может быть организована быстрая и удобная оплата штрафов ГИБДД по штрих-коду, расположенному на извещении.

Если торговая сеть заинтересована в увеличении трафика клиентов с различной покупательской способностью, то на кассах может быть организована оплата по штрих-коду коммунальных платежей и налогов.





Оплата товаров/услуг с мобильных телефонов

Востребованность мобильной коммерции как одного из наиболее доступных способов платежа растет с каждым годом. Карта «КиберСдача» позволяет оплатить покупку в магазине не только наличными и банковской картой, но и со счёта мобильного телефона.

1. Покупатель просит кассира провести оплату товара/услуги с карты «КиберСдача», привязанной к номеру мобильного телефона.
2. Кассир сканером считывает информацию со штрих-кода карты и вводит тип платежа и сумму. Эта информация, а также адрес и номер торговой точки в зашифрованном виде через систему «КиберПлат» (CyberPlat®) поступает сотовому оператору.
3. Сотовый оператор при достаточности средств на счёте абонента, если сумма платежа менее 1 000 рублей, отправляет ему USSD-запрос о подтверждении списания суммы. В ответ абонент со своего мобильного телефона отправляет «1» (согласен) или «0» (не согласен).
4. При сумме платежа свыше 1 000 рублей USSD-запрос требует введение PIN-кода.
5. В случае согласия абонента со счёта в режиме реального времени списываются средства в размере указанной суммы платежа.
6. Информация об этом поступает в торговую точку, и кассир, получив подтверждение, передаёт покупателю товар или проводит платёж за услугу и выдаёт чек.

КОМИССИОННАЯ ПОЛИТИКА

Для динамичного массового внедрения сервиса «КиберПлат» (CyberPlat®) используется гибкая комиссионная политика и не устанавливается единого стандартного тарифного плана для партнёров.

Размер внешней комиссии разработчик также не лимитирует: его величина устанавливается согласно договоренности эквайера карты и торговой сети.

Комиссия «активаторов» карт «КиберСдача» в первый год запуска сервиса фиксируется в размере 0,25% (включая НДС) со всего оборота по активированной карте в точках, не принадлежащих «активатору».

В дальнейшем размер комиссии может быть уменьшен. Доход эмитента от размещения рекламы на начальном этапе реализации в комиссионной политике не будет учитываться.

В SMS-сообщении, подтверждающем факт прохождения платежа, указывается сумма, зачисленная на счёт провайдера услуги.

ПРЕИМУЩЕСТВА ДЛЯ УЧАСТНИКОВ ПРОЕКТА

Преимущества для торговых сетей

- Увеличение объёма продаж за счёт покупателей, у которых кончились наличные денежные средства и отсутствуют банковские карты. Таким образом «КиберСдача» расширяет перечень платёжных инструментов у покупателя.
- Рост продаж, в первую очередь, недорогих и высокомаржинальных товаров, которые обычно располагаются в прикассовой зоне.
- Отсутствие дополнительных затрат вследствие использования готового высокотехнологичного решения.
- Высочайшая скорость оплаты, превосходящая время платежа с использованием банковской карты: вся операция занимает не более 6 секунд.
- Использование штрих-кода практически сводит к нулю вероятность введения ошибочных данных и, как следствие, исключает затраты на разбор ошибочных платежей.
- Снижение рисков работы с наличными денежными средствами.





ТЕХНОЛОГИИ ГЛОБАЛЬНОГО ЭЛЕКТРОННОГО БИЗНЕСА. МЕЖДУНАРОДНЫЕ ПРОЕКТЫ «КИБЕРПЛАТ» (CYBERPLAT®)

Преимущества для операторов мобильной связи

- Отсутствие каких-либо инвестиций.
- Опережение конкурентов во внедрении реально работающей мобильной коммерции.
- Создание имиджа супертехнологичной компании.
- Сведение к минимуму ошибок и, как следствие, снижение затрат на отмены и корректировки платежей.
- Сокращение времени операции, что позволит:
 - уменьшить расходы на приём платежей,
 - ускорить время приёма одного платежа.
- Рост остатков на счетах абонентов, что приводит к существенному увеличению пассива компании.
- Рост выручки, увеличение популярности, а следовательно, капитализации компании.

Преимущества участия для клиентов

- Покупатель получает новый удобный современный платёжный инструмент.
- Дополнительный психологический комфорт при оплате, так как в нашей стране доверие к операторам связи выше, чем к банкам.
- Максимальная безопасность: не надо произносить номер телефона вслух, списание средств подтверждается абонентом.
- Широчайшие возможности для пополнения лицевого счёта: торговая сеть существенно больше инфраструктуры приёма карт отдельного взятого банка.
- Скорость оплаты быстрее, чем при платеже по банковской карте.



CYBERPLAT INDIA — ОДИН ИЗ ЛИДЕРОВ НАЦИОНАЛЬНОГО ФИНТЕХРЫНКА

ОБЩИЕ СВЕДЕНИЯ

Один из самых крупных международных проектов «КиберПлат» (CyberPlat®) стартовал в Индии более 10 лет назад: компания CyberPlat India была основана в городе Мумбаи в 2009 году (www.cyberplat.in).

Развитие компании происходило стремительными темпами: несколько лет подряд CyberPlat India демонстрировал ежегодный 100%-ный прирост, уверенно опережая конкурентов.

В настоящее время CyberPlat India является одним из лидеров национальной финтехиндустрии. Компания входит в ТОП-5 платёжных систем, работающих на одном из крупнейших рынков Азии, и занимает 1-е место по количеству пунктов приёма платежей в стране: на 1 января 2019 года их число превышало 760 тысяч. Ежегодно в системе осуществляется более 240 миллионов транзакций в пользу более 350 поставщиков услуг в Индии и за её рубежами, доступных в 600 партнёрских сетях.

CyberPlat India один из немногих среди платёжных агрегаторов Индии напрямую сотрудничает более чем с двумя десятками крупнейших провайдеров, предоставляющих услуги в сфере телекоммуникаций, спутникового ТВ и ЖКХ.



Бизнес-модель

ПРОДУКТЫ И РЕШЕНИЯ

CyberPlat India предлагает партнёрам широкий спектр современных финансовых сервисов, востребованных жителями страны.

Пополнение счетов мобильных телефонов

CyberPlat India один из немногих среди платёжных интеграторов в стране имеет прямые шлюзы со всеми операторами связи и предлагает уникальный многофункциональный сервис пополнения лицевого счета операторов с использованием различных устройств.

Аппаратная многоплатформенность позволяет выбирать способ оплаты и осуществлять платежи с помощью компьютера, подключённого к интернету, веб-приложения, телефона на базе Android, банкомата или платёжного терминала самообслуживания.

Оплата спутникового ТВ

CyberPlat обладает самой масштабной инфраструктурой для сбора платежей за услуги всех провайдеров коммерческого телевидения (DTH), работающих в стране. Уникальные API и веб-платформы CyberPlat позволяют поставщику выбрать наиболее эффективный и маржинальный с точки зрения бизнеса вариант.

Постоплата мобильной и фиксированной связи

CyberPlat обеспечивает сбор платежей в пользу всех операторов мобильной и фиксированной связи, предоставляющих услуги как в стране, так и за её пределами. Партнёры CyberPlat получают важное конкурентное преимущество, предлагая в одной точке приёма платежей сразу весь спектр наиболее востребованных телекоммуникационных провайдеров.

Оплата провайдеров интернет-услуг

Пользователи интернета, число которых в стране превышает 283 миллиона человек, могут с максимальным удобством оплатить услуги интернет-провайдеров, выбрав способ платежа: онлайн или офлайн. Например, осуществить платёж можно на сайте партнёров CyberPlat или в близлежащем розничном магазине, и деньги мгновенно поступят на счёт.





Оплата страховых услуг

Оплата страховых взносов должна происходить в строго определенные сроки, и для этого у CyberPlat есть готовое эффективное решение, которое позволяет организовать сбор страховых премий разных компаний по принципу «одного окна».



Денежные переводы

Сервис денежных переводов является одной из наиболее востребованных услуг в Индии. Однако широкие слои населения, проживающие в сельских и полугородских районах, все ещё не имеют доступа к основным банковским услугам в связи с тем, что плотность охвата этих конгломератов банками по-прежнему очень низка.

Технологии CyberPlat позволяют решить эту проблему: они объединяют на единой API-платформе банковские сервисы и электронные кошельки и предоставляют возможность осуществлять денежные переводы в партнёрских торговых сетях.



Оплата подарочных карт

CyberPlat предлагает широчайший выбор товаров Топ-50 брендов Индии, объединённых на единой ИТ-платформе, предоставляя пользователям возможность выбрать в подарок то, что действительно им необходимо.

Оплата коммунальных услуг

Своевременная оплата коммунальных услуг — электричества и газа — крайне важна для жителей страны. CyberPlat предоставляет возможность удобной и быстрой оплаты услуг более 25 поставщиков этих энергетических ресурсов в точках приёма платежей, расположенных рядом с потребителями.



Business to Business

CyberPlat предлагает B2B-партнёрам различные модели дистрибуции и способы интеграции в формате онлайн и офлайн, которые в первую очередь адресованы:

- дистрибьюторским компаниям;
- e-commerce компаниям;
- стартапам;
- ритейлу;
- банкам;
- центрам обслуживания населения;
- сервисам поддержки.

МОДЕЛИ ДИСТРИБУЦИИ И СПОСОБЫ ИНТЕГРАЦИИ

- Розничная дистрибуция — доступ к более 500 тысяч пунктов приёма платежей партнёров CyberPlat.
- Дистрибуция в аграрных районах — доступ к «последней миле» через платёжную инфраструктуру CyberPlat, обладающую высокой степенью доступности в сельской местности.
- Современный розничный ритейл — реализация платёжных услуг в крупнейших современных розничных сетях, действующих в стране.
- Банковская инфраструктура — доступ к сетям банкоматов, банковским веб-порталам и мобильным приложениям.
- Электронная коммерция — сотрудничество с ведущими участниками рынка электронной коммерции.
- Мобильная коммерция — партнёрство с лидерами мобильной коммерции: в системе CyberPlat доступны все ключевые игроки национального рынка.
- Терминальные сети — интеграция услуг в крупнейшую в Индии сеть платёжных терминалов самообслуживания.
- Программы лояльности — широта выбора, лёгкость интеграции, гибкость настройки, оперативность.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ И ПАРТНЁРОВ

- Инновационные платёжные решения, которые применяются во многих странах мира, в том числе в России, Германии, Австрии.
- Возможность платежей с помощью различных устройств: компьютера, подключённого к интернету, веб-приложения, смартфона на базе ОС Android, банкомата, платёжного терминала.
- Полная безопасность платёжных операций: за все время работы не было ни одного взлома системы и проведения незаконных транзакций.
- Приём платежей в пользу трансграничных поставщиков услуг.
- Увеличение объёма высокомаржинальных операций.
- Приоритетное развитие наиболее востребованных населением сервисов.
- Расширение платёжной инфраструктуры в несколько раз в кратчайшие сроки и с минимальными затратами.
- Устойчивый и стабильный рост качественной клиентской базы.
- Укрепление лояльности существующих клиентов.

«КИБЕРПЛАТ КАЗАХСТАН» — ОСНОВОПОЛОЖНИК РЫНКА ЭЛЕКТРОННЫХ РАСЧЁТОВ В РЕСПУБЛИКЕ КАЗАХСТАН

ОБЩИЕ СВЕДЕНИЯ

Республика Казахстан стала первым зарубежным государством в рамках реализации стратегии глобального электронного бизнеса «КиберПлат» (CyberPlat®), в котором компания успешно осуществила проект создания масштабной платёжной инфраструктуры. «КиберПлат Казахстан» была основана 15 сентября 2005 года, а первый электронный платёж в этой стране через систему «КиберПлат» (CyberPlat®) был осуществлён в апреле 2006 года.

Развитие компании происходило стремительными темпами. В короткие сроки в стране была создана обширная инфраструктура приёма розничных платежей, позволяющая населению быстро и удобно оплачивать наиболее востребованные услуги. В настоящее время платёжная сеть «КиберПлат» (CyberPlat®) на территории Казахстана насчитывает более 20 тысяч точек.

«КиберПлат Казахстан» предлагает партнёрам возможность пополнения счетов с помощью различных устройств: компьютера, подключённого к интернету, веб-приложения, смартфона на базе ОС Android, банкомата, платёжного терминала самообслуживания.

Работа системы отличается высочайшей надёжностью и устойчивостью к сбоям. Система базируется на двух процессинговых центрах на территории Казахстана, связь между которыми дублируется через сети независимых провайдеров. Такая



Общая схема бизнеса

схема резервирования в сочетании с современной кластерной архитектурой обеспечивает высокую отказоустойчивость и независимость от форсмажорных обстоятельств.

Гарантируется полная безопасность платёжных операций: за все время работы в стране не было ни одного взлома транзакции.

Высокое качество сервиса «КиберПлат» (CyberPlat®) и его неоспоримые технологические преимущества способствуют дальнейшему интенсивному развитию рынка электронных расчётов в Казахстане.

КЛИЕНТСКАЯ БАЗА

Провайдеры услуг

Успешное развитие высокотехнологичного бизнеса в Казахстане сразу же привлекло внимание ведущих игроков национального рынка, быстро оценивших эффективность сотрудничества с лидером рынка электронных финансов.

«КиберПлат Казахстан» имеет платёжные шлюзы ко всем ведущим операторам мобильной связи, интернет-провайдерам, поставщикам коммунальных услуг, энергосбытовым компаниям, банкам, микрофинансовым организациям, MLM-операторам, букмекерским конторам и другим провайдерам услуг. Компания также

Сотовая связь	 Beeline™	 Kcell	 ACTIV	 ALTEL		и другие
Фиксированная связь	 Beeline™	 MegaTel		 TRANSTELECOM		и другие
Коммунальные платежи						и другие
Интернет, ТВ						и другие
Российские сотовые операторы стран СНГ						и другие
Букмекерские конторы						и другие
Сетевой маркетинг						и другие
Трансграничные услуги						и другие



осуществляет приём платежей в адрес трансграничных поставщиков. Общее число провайдеров превышает 300 компаний и организаций.

Партнёрами системы электронных платежей являются компании с масштабным охватом территории: сети салонов сотовой связи, магазины

электроники и бытовой техники, крупнейшие терминальные сети и другие представители различных отраслей бизнеса Республики Казахстан.

Одной из ключевых вех в развитии платёжной инфраструктуры страны стал совместный проект «КиберПлат Казахстан» с АО «Казпочта» — национальным оператором почтовой связи с разветвленной сетью из 3200 отделений.

Банки-партнёры

В число партнёров компании входят значимые федеральные и отраслевые банки, работающие на всей территории Казахстана. «КиберПлат» (CyberPlat®) последовательно развивает сотрудничество, предлагая современные финансовые сервисы пополнения банковских счетов, погашения потребительских кредитов, пополнения карт международных платёжных систем и масштабную республиканскую платёжную сеть для оплаты клиентами банков самых различных услуг.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ И ПАРТНЁРОВ

Партнёры «КиберПлат Казахстан» высоко ценят возможности сотрудничества с лидером платёжной отрасли страны, определяя в качестве значимых следующие позитивные факторы в организации бизнеса:

- инновационные платёжные решения, которые применяются в разных странах мира;
- устойчивый и стабильный рост качественной клиентской базы;
- укрепление лояльности существующих клиентов;
- расширение платёжной инфраструктуры в кратчайшие сроки и с минимальными затратами;
- увеличение объёма высокомаржинальных операций;
- широкий и постоянно обновляемый перечень сервисов;
- приоритетное развитие наиболее востребованных населением платёжных услуг;
- мультиплатформенность платёжных решений: возможность платежей с помощью различных устройств;
- высочайшая отказоустойчивость и независимость от форс-мажорных обстоятельств благодаря современной надёжной IT-архитектуре с кратным запасом прочности ресурсов;
- полная безопасность платёжных операций: за всё время работы системы не было ни одного взлома и проведения незаконных транзакций.

ИННОВАЦИОННЫЕ СЕРВИСЫ «КИБЕРПЛАТ» (CYBERPLAT®) ДЛЯ ЗАРУБЕЖНЫХ ОПЕРАТОРОВ СВЯЗИ

ПРЕДЛОЖЕНИЯ ДЛЯ ЗАРУБЕЖНЫХ ОПЕРАТОРОВ СВЯЗИ

В рамках глобальной экспансии на мировой рынок электронных финансовых услуг одним из приоритетов «КиберПлат» (CyberPlat®) является сотрудничество с крупнейшими игроками в сегменте телекоммуникационных сервисов.

«КиберПлат» (CyberPlat®) предлагает зарубежным провайдерам связи:

- успешный 20-летний опыт эффективной организации приёма платежей;
- эффективную технологию обработки транзакций, превышающую в 10 раз аналогичные продукты конкурентов;
- проактивную стратегию интенсивного развития;
- доступность сервисов во многих странах;
- 4-кратный резерв технологических возможностей процессинга;
- высококвалифицированную команду IT разработчиков и финансовых экспертов.

АППАРАТНАЯ МНОГОПЛАТФОРМЕННОСТЬ

Одним из ключевых конкурентных преимуществ, которые система «КиберПлат» (CyberPlat®) обеспечивает зарубежным партнёрам, является свобода выбора способа оплаты и использование различных устройств для проведения платежа в зависимости от требований партнёров.

Оплата может происходить с использованием:

- компьютера или смартфона;
- кассового аппарата;
- pos-терминала;
- платёжного терминала самообслуживания;
- банкомата;
- интернет-Банк-Клиента;
- мобильной витрины.

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ

Технология «КиберПлат» (CyberPlat®) обеспечивает абсолютную безопасность финансовых транзакций и минимизирует количество ошибочных платежей. В рамках одной транзакции в системе совершается до 16 операций, заверенных электронной подписью, и используются защищённые способы передачи данных по интернет-каналам. Они включают в себя проверку наличия номеров телефонов или лицевых счетов клиентов в биллинговых системах провайдеров услуг, идентификацию и авторизацию точек приёма платежей и другие операции, гарантирующие безопасность транзакции. В системе «КиберПлат» (CyberPlat®) за всё время работы не произошло ни одного случая взлома транзакции.

ПРЕИМУЩЕСТВА «КИБЕРПЛАТ» (CYBERPLAT®) ПЕРЕД ДРУГИМИ ПЛАТЁЖНЫМИ ТЕХНОЛОГИЯМИ

Исторически основным конкурентом платёжных технологий «КиберПлат» (CyberPlat®) во многих странах являются карты экспресс-оплаты, или скретч-карты. Этот финансовый продукт представляет собой эквивалент денежных средств, используемый при пополнении лицевых счетов абонентов мобильной связи. Скретч-карты более всего востребованы в сегменте платежей от \$5 до \$25, которые оказываются нерентабельными при оплате услуг связи в банковской инфраструктуре.

Несмотря на определённую востребованность скретч-карт, они обладают рядом очевидных недостатков:

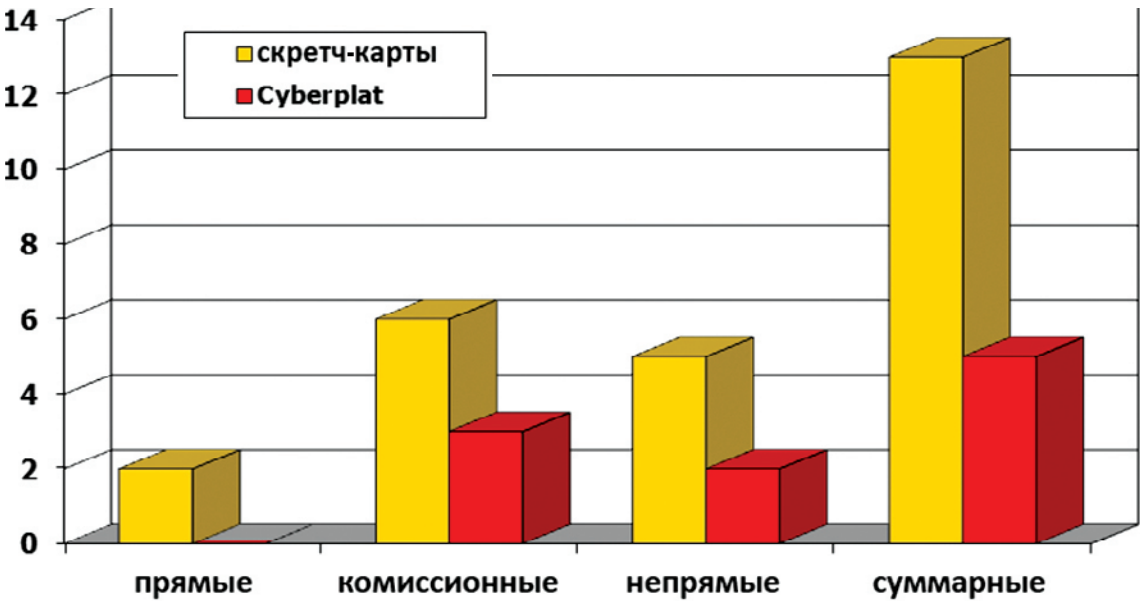
- высокая стоимость производства;
- предустановленный номинал карты;
- большой временной промежуток между заказом на производство и активацией карт;
- избыток регистрационных кодов доступа (закрытых и открытых, штрих-кодов);
- короткое «время жизни» карты у пользователя — в 99% случаев оно составляет 5–10 минут;
- невозможность активации скретч-карты на другой номер телефона.

Затраты операторов

Прямые издержки операторов мобильной связи при использовании скретч-карт довольно велики и достигают 12%.

Они складываются из следующих видов расходов:

- внешние затраты (составляют около 2%);
- производство карты — около \$0,2 за карту;
- затраты на содержание персонала производственного и коммерческого подразделений;
- затраты на содержание персонала финансовых подразделений;



Сравнение затрат: «КиберПлат» (CyberPlat®) vs. скретч-карты

- затраты на ответственное хранение карт;
- затраты на контроль за работой персонала в месте продаж (staff's fraud);
- затраты на защиту от подделок;
- затраты на инкассацию;
- комиссия дилера (составляет около 6%).

Непрямые затраты оператора зависят от торговой наценки розничной сети, где реализуются скретч-карты, и обычно составляют порядка 5%. Другими словами, в 95% ритейла карта номиналом \$10 должна продаваться за \$10,5, и, таким образом, абонент за получение мобильных услуг вынужден платить 5%-ную комиссию.

Очевидно, что абонент предварительно рассчитывает, сколько денежных средств готов заплатить, и старается избегать дополнительных расходов. Вот почему он предпочтёт вместо покупки скретч-карты номиналом \$10 за \$10,5 оплатить именно нужную сумму через систему «КиберПлат» (CyberPlat®). Провайдер, в свою очередь, сможет получить всю внесенную абонентом сумму.

Прямые издержки при оплате в системе «КиберПлат» (CyberPlat®) складываются из внешних затрат провайдера на персонал, разработавший платёжный шлюз (обычно 5–7 человек в IT-департаменте) и занимающийся его технической поддержкой. Суммарно объём затрат не превышает 0,01% оборота и всегда может быть ещё более приближен к нулевому значению.

Ещё одна статья расходов — это комиссия, выплачиваемая системе «КиберПлат» (CyberPlat®). В первый год работы комиссия составляет 3%, а в последующие уменьшается до 2%.

При использовании системы электронных платежей «КиберПлат» (CyberPlat®) операторы мобильной связи могут уменьшить прямые и непрямые затраты в среднем на 5–13%.

	Скретч-карты (только предоплаченная услуга)	«КиберПлат» (CyberPlat®) (любой тарифный план)
Шаг 1	Найти точку продаж, где есть карта требуемого номинала	Найти точку приёма платежей «КиберПлат» (CyberPlat®)
Шаг 2	Купить карту требуемого номинала	Пополнить счёт на любую сумму на любой номер телефона
Шаг 3	Позвонить в систему активации карт	Нет
Шаг 4	Ввести PIN-код (12–16 цифр) с клавиатуры телефона	Нет
Шаг 5	Убедиться в пополнении баланса телефона	Убедиться в пополнении баланса телефона
Риски	Покупка подделки, просроченной карты или её потеря	Нет

Использование технологий «КиберПлат» (CyberPlat®) способствует повышению качества абонентской базы оператора и укреплению лояльности пользователей услуг, снижает вероятность оттока клиентов, а также уменьшает затраты на привлечение новых абонентов.

По оценкам экспертов, благодаря только этим преимуществам «КиберПлат» (CyberPlat®) прирост абонентской базы у зарубежных операторов связи может составить 8–10%, а в случае комплексной интеграции — достигнуть 20%.

**ПРЕИМУЩЕСТВА ОТ ВНЕДРЕНИЯ ПЛАТЁЖНЫХ РЕШЕНИЙ
«КИБЕРПЛАТ» (CYBERPLAT®)**

- Полное исключение расходов, связанных с производством и поддержкой технологий скретч-карт (экономия затрат — более 10%).
- Снижение общих затрат на сопровождение бизнеса.
- Увеличение количества мелких платежей (\$5 и менее), составляющих большую часть, что способствует росту оборота компании до 10%.
- Рост клиентской базы (до 20%).
- Уменьшение длительности «периода молчания» абонентов.
- Увеличение объёма продаж (до 20%) благодаря росту трафика плательщиков, привлечённых удобством платежей в торговых точках с сервисом «КиберПлат» (CyberPlat®).
- Дополнительные доходы за счёт зачисления сдачи от покупок на счёт мобильного телефона на кассах торговых точек.
- Рост прибыли и увеличение рыночной стоимости компании.

КОНТАКТЫ

ООО «КИБЕРПЛАТ»

ЦЕНТРАЛЬНЫЙ ОФИС:

123610, г. Москва, Центр Международной Торговли, Краснопресненская наб., д. 12, подъезд 7, этаж 12

Телефон: +7 (495) 967-02-20,
факс: +7 (495) 967-02-08

e-mail: info@cyberplat.ru,
sales@cyberplat.ru,
market@cyberplat.ru

skype: CyberPlat

www.cyberplat.ru

Служба технической поддержки:

Телефоны: +7 (495) 981-80-80,
+7 (495) 967-02-20

e-mail: help@cyberplat.ru,
support@cyberplat.ru

skype: support_cyberplat

Региональные дирекции:

Средняя Волга (Самара)
моб. +7 (960) 808-39-70
e-mail: samara@cyberplat.ru

Центральное Черноземье (Курск)
моб. +7 (910) 210-81-84
e-mail: kursk@cyberplat.ru

Урал (Екатеринбург)
тел./факс +7 (343) 379-01-65
моб. +7 (922) 228-76-48
г. Екатеринбург, ул. Фронтových
Бригад, д. 18а, к. 308
e-mail: ekaterinburg@cyberplat.ru

Юг (Ставропольский край)
моб. +7 (928) 815-52-08
e-mail: stavropol@cyberplat.ru

Дочерняя компания в Казахстане:

ТОО «КИБЕРПЛАТ КАЗАХСТАН»
Республика Казахстан,
050000, г. Алматы,
ул. Гоголя, д. 84а, офис 201

Телефоны: +7 (727) 2-500-861,
+7 (727) 2-663-951,
+7 (727) 2-508-563,
+7 (777) 2-780-006

(бесплатно с номеров Beeline)

Факс: +7 (727) 2-508-564 (доб. 107)

e-mail: info@cyberplat.kz

www.cyberplat.kz

Дочерняя компания в Индии:

Stylus Serviced Offices, 801,
8th Floor, A-Wing, Reliable Tech Park,
Behind Reliable Plaza, Off Thane Belapur
Road, Airoli, Navi Mumbai — 400 708

Business Enquiries: +91-22-30114605,
+91-22-30114604

Support Numbers: +91-9004-66-3334,
+91-9004-66-3339

E-mail: help@cyberplat.in

Skype: helpdesk.cyberplatindia

http://www.cyberplat.in

ПРИЛОЖЕНИЕ

CYBERCHECK

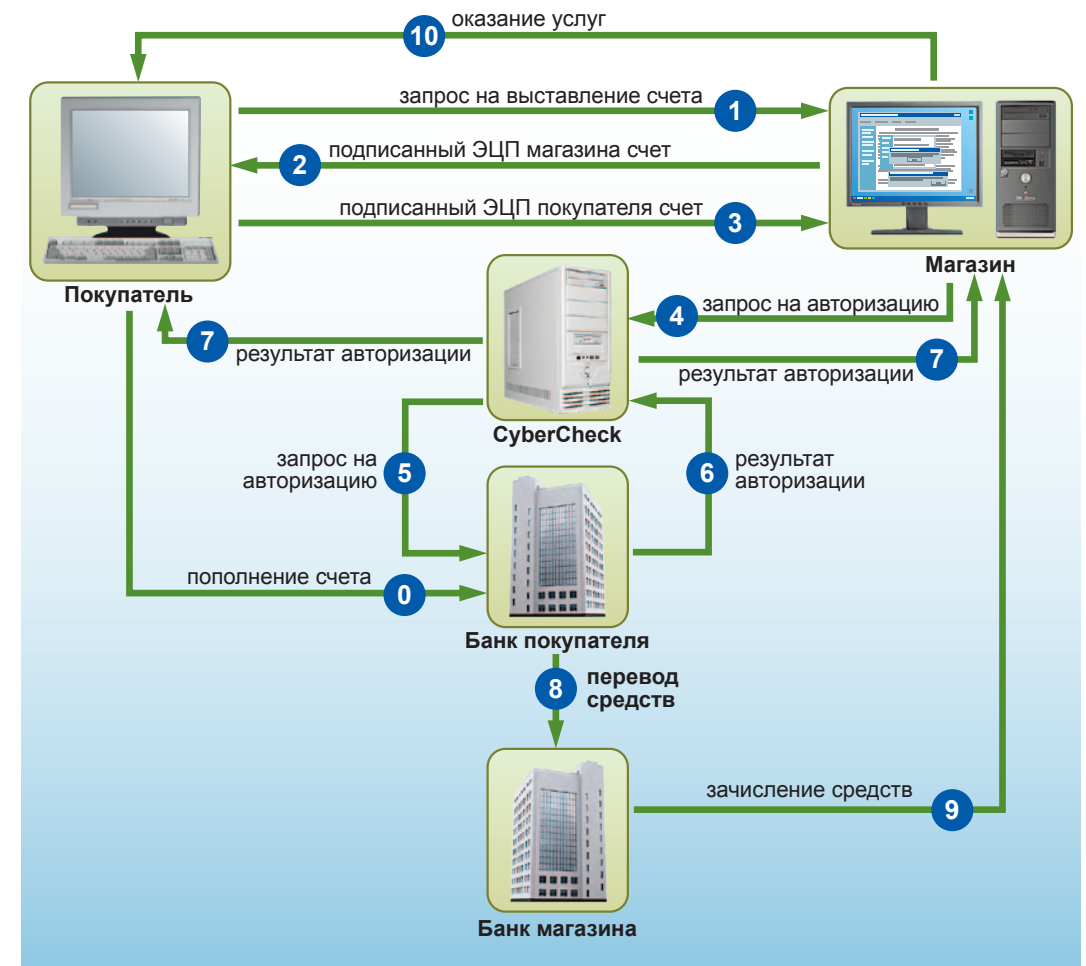
1. Покупатель через интернет подключается к веб-серверу Магазина, формирует корзину товаров и направляет Магазину запрос на выставление счёта.
 2. Магазин в ответ на запрос Покупателя направляет ему подписанный своей электронной подписью (ЭП) счёт, в котором указывает:
 - наименование товара (услуги);
 - стоимость товара (услуги);
 - код магазина;
 - время и дату совершения операции.
- С гражданско-правовой точки зрения этот счёт является предложением заключить договор (офертой).

1. Покупатель подписывает своей ЭП предъявленный ему счёт и отправляет его, в свою очередь, в Магазин, акцептуя тем самым оферту (договор). Договор считается заключённым с момента подписания Покупателем выставленного ему счёта. В системе счёт, подписанный Покупателем, становится чеком.
2. Подписанный двумя ЭП (Магазином и Покупателем) чек направляется Магазином на Авторизационный сервер CyberCheck для авторизации.
3. CyberCheck проводит проверку подписанного чека:
 - проверяет наличие в Системе Магазина и Покупателя;
 - проверяет ЭП Покупателя и Магазина;
 - сохраняет копию чека в базе данных CyberCheck.

В случае положительного результата проверки чек отправляется в Банк Покупателя (Банк-Участник системы, в котором ведется счёт клиента-Покупателя в системе «КиберПлат» (CyberPlat®)) для проведения платежа.

Банк Покупателя проверяет остаток и лимиты средств на счёте Покупателя. В результате проверки формируется разрешение на проведения платежа или его запрет. Банк Покупателя передаёт результат авторизации CyberCheck.

6. При разрешении платежа:
 - CyberCheck передаёт Магазину разрешение на оказание услуги (отпуск товара);
 - Банк Покупателя переводит денежные средства со счёта Покупателя в Банк Магазина (Банк-Участник системы, в котором ведутся счета клиентов-Магазинов в системе «КиберПлат» (CyberPlat®));
 - Банк Магазина зачисляет денежные средства на счёт Магазина;
 - Магазин оказывает услугу (отпускает товар).
7. При запрете платежа:
 - CyberCheck передаёт Магазину отказ от проведения платежа;
 - покупатель получает отказ с описанием причины.



Покупатель полностью контролирует процесс совершения покупки. В качестве документального подтверждения совершённой сделки у каждой стороны остаются подписанные ЭП чеки, удостоверяющие факт совершения сделки и имеющие юридическую силу.

Выписка по счёту

1. Покупатель запрашивает выписку о состоянии своего счёта, подписывая запрос своей ЭП.
2. CyberCheck проверяет код Покупателя и его ЭП.
3. При положительных результатах проверки CyberCheck направляет Банку запрос на выписку, получает выписку и перенаправляет её Покупателю в виде криптографически преобразованного текста с ЭП CyberCheck.
4. Покупатель получает сообщение, проводит проверку подписи CyberCheck и обратное криптографическое преобразование выписки.
5. Покупатель сохраняет выписку на своем компьютере.

Запрос о прохождении платежей Покупателя в Магазине

1. Покупатель запрашивает информацию о проведённых им в данном Магазине платежах, указывая свой код в системе «КиберПлат» (CyberPlat®).
2. На основании полученного кода Магазин предоставляет информацию о платежах данного Покупателя.

СУБЕРСЧЕК С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАСТИКОВЫХ КАРТ

Регистрация держателя пластиковой карты

1. Держатель пластиковой карты МИР, VISA или MasterCard (далее — Покупатель) регистрируется в системе электронных платежей «КиберПлат» (CyberPlat®).
2. При регистрации Покупатель указывает:
 - свои персональные данные (фамилию, имя, отчество, паспортные данные, адрес электронной почты, почтовый адрес, телефон);
 - параметры своей карточки (название платёжной системы, в которой зарегистрирована карта; номер карты; дату окончания действия карты; имя держателя карты в транскрипции, использованной на карте).

Информация о карте передаётся в защищённом виде только на сервер CyberCheck системы электронных платежей «КиберПлат» (CyberPlat®) при регистрации Покупателя и не предоставляется Магазину при операциях Покупателя.

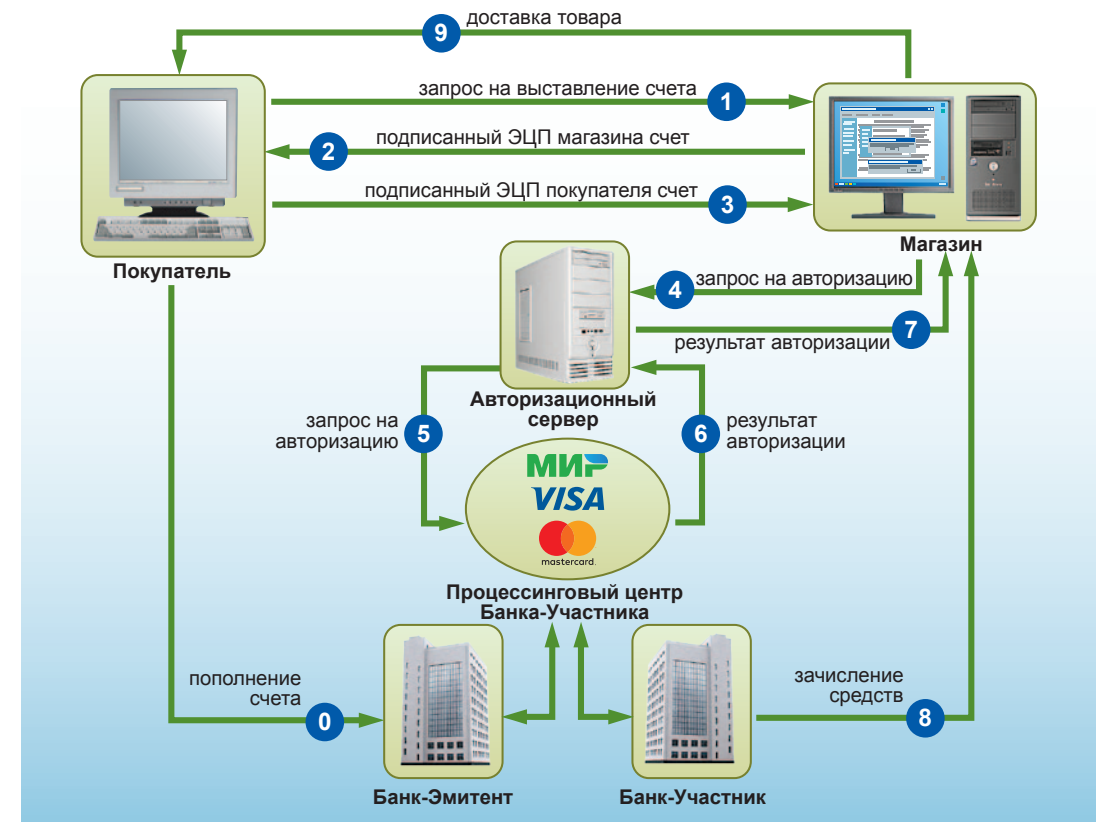
Онлайн-покупка и проведение платежа

Процедура покупки товаров в Магазинах осуществляется по технологии «КиберПлат» (CyberPlat®).

1. Покупатель через интернет подключается к веб-серверу Магазина, формирует корзину товаров и направляет Магазину запрос на выставление счёта.
2. Магазин в ответ на запрос Покупателя направляет ему подписанный своей ЭП счёт, в котором указывает:
 - наименование товара (услуги);
 - стоимость товара (услуги);
 - код магазина;
 - время и дату совершения операции.

С гражданско-правовой точки зрения этот счёт является предложением заключить договор (офертой).

3. Покупатель подписывает своей ЭП предъявленный ему счёт и отправляет его, в свою очередь, в Магазин, совершая тем самым акцепт оферты (договора). Договор считается заключённым с момента подписания Покупателем выставленного ему счёта. В системе, счёт, подписанный Покупателем, становится чеком.
4. Подписанный двумя ЭП (Магазина и Покупателя) чек направляется Магазином на CyberCheck для авторизации.
5. CyberCheck проводит проверку подписанного чека:
 - проверяет наличие в системе Магазина и Покупателя;
 - проверяет ЭП Покупателя и Магазина;
 - сохраняет копию чека в базе данных CyberCheck.



6. При отрицательном результате проверки:
 - CyberCheck передаёт Магазину отказ от проведения платежа;
 - Покупатель получает отказ с описанием причины.
7. При положительном результате проверки:
 - чек перенаправляется серверу CyberPOS для формирования авторизационного запроса;
 - CyberPOS передаёт его в процессинговый центр Банка-Участника;
 - запрос на авторизацию передаётся через закрытые банковские сети Банку — Эмитенту карточки Покупателя или процессинговому центру карточной платёжной системы, уполномоченному Банком-Эмитентом.
8. При положительном результате авторизации, полученном от карточной платёжной системы:
 - Процессинговый центр Банка-Участника передаёт CyberPOS положительный результат авторизации;
 - CyberPOS передаёт CyberCheck положительный результат авторизации;
 - CyberCheck передаёт Покупателю положительный результат авторизации;
 - CyberCheck передаёт Магазину разрешение на оказание услуги (отпуск товара);
 - Магазин оказывает услугу (отпускает товар);
 - Банк-Участник зачисляет средства на счёт Магазина в соответствии с существующими договорными отношениями между Банком-Участником и Магазином.

9. При отказе в авторизации:

- Процессинговый центр передаёт CyberPOS отказ от проведения платежа;
- CyberPOS передаёт CyberCheck отказ с описанием причины;
- CyberCheck передаёт Покупателю отказ с описанием причины;
- CyberCheck передаёт Магазину отказ от проведения платежа.

Покупатель полностью контролирует процесс совершения покупки. В качестве документального подтверждения совершённой сделки у каждой стороны остаются подписанные ЭП чеки, удостоверяющие факт совершения сделки и имеющие юридическую силу.

Выписка по счёту

1. Покупатель запрашивает выписку о состоянии своего счёта, подписывая запрос своей ЭП.
2. CyberCheck проверяет код Покупателя и его ЭП.
3. При положительных результатах проверки CyberCheck направляет Банку запрос на выписку, получает выписку и перенаправляет её Покупателю в виде криптографически преобразованного текста с ЭП CyberCheck.
4. Покупатель получает сообщение, проводит проверку подписи CyberCheck и обратное криптографическое преобразование выписки.
5. Покупатель сохраняет выписку на своём компьютере.

Запрос о прохождении платежей Покупателя в Магазине

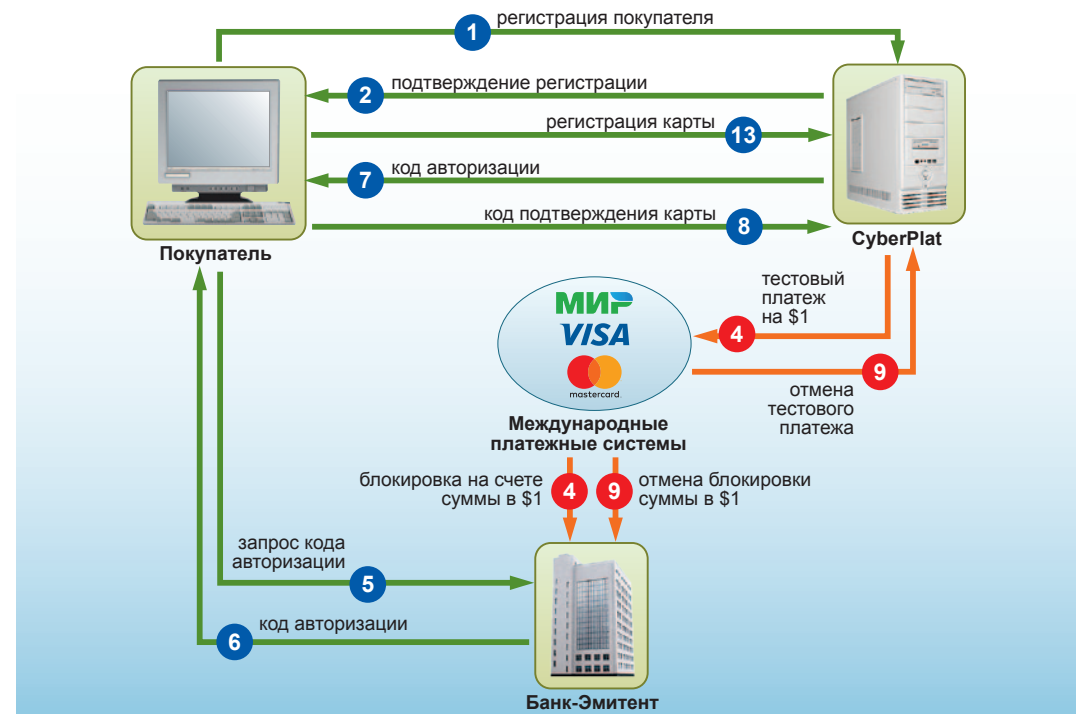
1. Покупатель запрашивает информацию о проведённых им в данном Магазине платежах, указывая свой код в системе «КиберПлат» (CyberPlat®).
2. На основании полученного кода Магазин предоставляет информацию о платежах данного Покупателя.

CYBERPLATPAY

Для повышения безопасности интернет-платежей система «КиберПлат» (CyberPlat®) предлагает магазинам и покупателям новую технологию CyberPlatPay. Технология CyberPlatPay обеспечивает возможность подтверждения покупателем при интернет-платежах прав на использование пластиковой карты. Это, с одной стороны, увеличивает доверие Магазина к платежам Покупателя по кредитным картам и, с другой стороны, даёт Покупателю дополнительные гарантии надёжности совершения покупки.

Для подтверждения своих полномочий законного держателя пластиковой карты Покупатель должен пройти и регистрацию в CyberPlatPay, которая осуществляется следующим образом.

1. Покупатель — держатель пластиковой карты регистрируется в CyberPlatPay, внося свои персональные данные.
2. Система формирует персональный раздел Покупателя и выдаёт сообщение о подтверждении регистрации.
3. Покупатель начинает регистрацию своей пластиковой карты (персональный раздел — регистрация карты). Для этого он входит в свой персональный раздел и вносит в систему реквизиты карты. Система формирует тестовую



транзакцию (тестовый платёж) на сумму \$1 (эта сумма по завершении процесса регистрации будет возвращена Покупателю вне зависимости от результатов регистрации).

4. Транзакция передаётся в соответствующую платёжную систему, и на счёте Покупателя в Банке-Эмитенте карты блокируется (холдируется) \$1.
5. Покупатель связывается с обслуживающим его Банком-Эмитентом и запрашивает код авторизации тестового платежа.
6. Банк, удостоверив личность Покупателя, сообщает ему код авторизации.
7. Полученный код авторизации передаётся клиентом в CyberPlatPay (персональный раздел — информация о картах).
8. CyberPlatPay проверяет истинность переданного кода и тем самым законность использования пластиковой карты. Система CyberPlatPay формирует код подтверждения карты (пароль) для использования пластиковой карты и сообщает его Покупателю.
9. Система «КиберПлат» (CyberPlat®) формирует распоряжение об отмене тестового платежа и передаёт его в платёжную систему. Заблокированная на счёте Покупателя сумма в \$1 освобождается.

Полученный Покупателем код подтверждения карточки используется при реальных платежах — он сообщается наряду с другими реквизитами карты и проверяется системой CyberPlatPay. Для этого Покупателю на странице ввода карточных данных необходимо отмечать, что он платит по зарегистрированной карте, и указывать код подтверждения.

Использование зарегистрированных пластиковых карт позволяет установить более высокий уровень доверия между Покупателем, интернет-магазином и системой электронных платежей «КиберПлат» (CyberPlat®).

РИСК-МЕНЕДЖМЕНТ КРИПТОВАЛЮТ

Впервые вопрос о блокчейне встал передо мной, после того, как Герман Оскарович Греф выступил в 2014 году на Давосском форуме. Меня тогда спросили, что такое биткоин, а я им никогда не занимался, и ответить мне было нечего. Даже стало досадно: как это, Герман Оскарович Греф знает, а я нет? Тем более, что мы с ним в 2010–2011 годах весьма долго говорили о технологиях (он хотел купить «Киберплат», но мы не договорились), и объем его познаний в цифровых технологиях я представляю очень хорошо.

Я занимаюсь компьютерами с 1983 года без перерывов и глубоко нахожусь в этой теме. А он, в общем-то, гуманитарий, и его взгляд в ИТ вряд ли может быть более глубоким. Чего, например, стоит идея в своем университете обучить сотрудников Сбербанка математическому инструменту искусственного интеллекта?! Я немножко занимался искусственным интеллектом в 1988–1989 годах и отлично знаю, что для этого надо сначала изучить математический анализ, линейную алгебру, теорию вероятностей, математическую статистику, методы моделирования, методы алгоритмизации... и только потом заняться только азами искусственного интеллекта! Не всякий отличник с крепким техническим образованием такое воспримет, а гуманитарий тем более: это приблизительно как революционного матроса обучать различиям в технике живописи импрессионистов.

Тем не менее, я начал разбираться в том, что такое биткоин, и пришел к печальному выводу. Почему печальному? Большинство радостно говорит нам: «Все туда идут, все там деньги зарабатывают!» Но в отличие от большинства, я знаю,

Попробую вам объяснить это понятие максимально популярно, без профильных тонкостей. Возьмем, например, страховой бизнес. Как формируются страховые премии по риску угона автомобиля? Страховщики смотрят статистику угонов определенной марки автомобилей за прошлый год. Допустим, угоняли 3% машин... Они предлагают ставку 4% и знают, что если застрахуют 100 машин, то три автомобиля угонят, а премия по четвертому останется им, и они все равно заработают себе на автомобиль. В этом и состоит оценка риска — знать величину риска максимально точно. А если после получения хороших премий еще и попробовать «угговорить» угонщиков не заниматься угонами — это уже риск-менеджмент.

В банковском бизнесе оценка риска обычно представлена в виде процентных ставок. Когда в банк приходит потенциальный заемщик, банкиры рассчитывают ему риски: страновой риск стоит столько-то, риск на правовую систему столько-то, риск на отрасль экономики, риск на собственника, риск на развитие технологий... Все это складывается в итоговую ставку по кредиту — например, 12,5% годовых. И клиенту показывают, почему именно столько, а не, например, 10% и не 15%.

Так же надо считать риски и в новых технологиях. Когда финансисты и/или аййтишники профессионально «заходят» в новую область, они обязательно создают риск-менеджмент новой области: эдакую условную книгу, где оглавление — это перечень рисков, и каждая глава - это описание риска как такового, его граничные величины и методы его минимизации.

Давайте посмотрим, как подобные ситуации решались раньше. Например, для управления кредитными рисками банкиры привлекали юристов, разрабатывали длинные кредитные договоры, потом понимали, что нужно иметь какое-то обеспечение этих кредитных рисков... Кредитование в том виде, в каком есть сейчас, началось совсем не сразу! Банкам как институции всего 400-500 лет, и за эти 500 лет были придуманы такие инструменты, как юридическое сопровождение кредитных договоров, варианты обеспечения, гарантии, поручительства, залоги и т.д. и т.п.

ЧТО ТАКОЕ РИСК-МЕНЕДЖМЕНТ



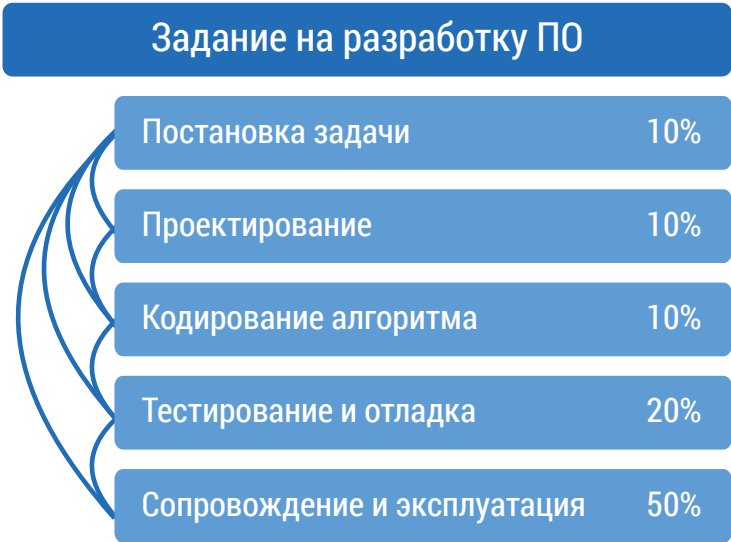
Существуют расчетные риски. Для их преодоления лицензируют предприятия, занимающиеся расчетами. Не все подряд занимаются расчетами массово, а только те, за кем Центральный Банк регулярно приглядывает. Когда придумали чеки, по ним со временем сделали целое законодательство. По аккредитивам — тоже, по счетам эскроу — тоже.

История создания риск-менеджмента кредитных и расчетных рисков показывает, что решать вопросы риск-менеджмента блокчейна, биткойна и различных криптовалют вполне возможно. А решение, как обычно, трехэтапное: перечисление рисков, описание рисков (модель угрозы), работа по нахождению методов минимизации рисков.

Где мы сейчас находимся в риск-менеджменте криптовалют

Прежде всего, пока в России, да и в мире, наблюдается низкое понимание происхождения этой технологии и целей ее создателей. Наталья Касперская начала немного рассказывать про американское происхождение биткойна, но большинство людей в принципе не понимает, кто и зачем это создал. Каково было техническое задание на разработку, если получился такой результат? Почему из огромного многообразия вариантов создатели выбрали именно такие технологические принципы?

Беда неграмотной оценки влияния технологии на жизнь часто состоит в максималистских оценках, проистекающих из того, что такой неграмотный оценщик даже приблизительно не представляет, о чем рассуждает. Есть одна оценка: вся наша жизнь глобально изменится, потому что пришел блокчейн. И есть другая: трогать это не надо, потому что криптовалюты — организованное мошенничество. Представляете, какой разрыв? Это даже не ситуация, когда вы заходите в темную комнату и не знаете, слон там или кошка. Это ситуация, когда вы не уверены, в комнате ли вы вообще.



Этапы разработки программного обеспечения

В КАКОЙ ПЛОСКОСТИ НАХОДЯТСЯ РИСКИ КРИПТОВАЛЮТ?

Поэтому, когда я начал изучать криптовалюты, я начал смотреть именно на перечень рисков... И обнаружил, что их не только много, а они еще и находятся в трех больших и разных плоскостях: риски айтишные, риски экономические, риски юридические. И найти одного универсального специалиста, который разобрался бы сразу во всех этих направлениях, практически невозможно. Таких людей — десяток на страну, и вряд ли они работают чиновниками.

Поэтому, по большому счету, прежде чем заниматься криптовалютой, нужно составить список всех рисков, какие только возможны, и разделить их на профессионально-ориентированные группы рисков, где каждую разберет соответствующий специалист. Юридическую группу рисков — юрист, экономическую группу рисков — экономист, и так далее. Потому что когда экономист начинает рассуждать об айтишных рисках, ничего хорошего не выходит. В этом самая главная проблема всех цифровых валют: каждый говорит о своем, и никому не пришло в голову, что нужно всем, кто хочет этим заниматься, собраться вместе, создать общество, состоящее из отделов по профилям, которое каждый риск относил бы к компетенции того или иного отдела.

Первый вывод заключается в том, что основная проблема анализ блокчейн-технологий, а правильнее было бы сказать технологий распределенного реестра, требует детальной компетенции в разных областях.

Что это за области?

Во-первых, это общая электроника, или понимание того, как вообще работают компьютеры. Надо понимать, почему она основана на двоичной системе счисления (именно единичках и ноликах), а не на, условно говоря, двоечках или троечках.

Далее, очень важна новейшая электроника, она же электроника так называемых «закрытых» областей, прежде всего - военная электроника, в которой применяются специальные алгоритмы. Ведь сугубо мирных технологий изначально не бывает. Если человек что-то изобретает, обычно это изобретение сначала используется для того, чтобы всех соперников поубивать. Когда человечеству удалось осуществить расщепление атомного ядра, для начала

Требуется детальная компетенция (включающая многолетний опыт) в разнопрофильных направлениях

- Электроника общая
- Электроника «закрытых» областей
- Юриспруденция публичного права
- Юриспруденция частного (торгового) права
- Макроэкономика

Специалистов, одновременно компетентных во всех перечисленных сферах, очень мало. Чиновников, имеющих право готовить или принимать решения одновременно во всех перечисленных сферах, не существует.

Основная проблема анализа блокчейн-технологий

убили 300 тысяч человек в Хиросиме и Нагасаки. Думаю, что и обезьяна взяла палку в первый раз не для того, чтобы фрукт сбить с дерева, а чтобы настучать по голове другой обезьяне.

То же самое в электронике — все, что мы видим в мирной области, будьте уверены, сначала использовалось в военной. Например, сотовая связь — это полевая опорная сеть связи, разработанная еще в середине XX века для военного применения. Часть этой технологии рассекретили, и она стала доступна обычным абонентам. Интернет изначально назывался ARPANET и связывал между собой несколько сотен военных учреждений и предприятий в США. Его рассекретили, передали в открытое пользование — теперь мы шлем друг другу электронные письма, смотрим новостные и прочие сайты.

Итак, для анализа технологий распределенного реестра нужны как минимум базовые знания в электронике двух видов.

Далее — юриспруденция. Юриспруденцию нужно знать и публичного права: каким образом криптовалюты, деньги, расчеты регулируются государством, и частного (торгового) права, то есть как два равноправных лица (юридических или физических) могут ими обмениваться.

И, конечно же, знать макроэкономику. Попробуйте представить, как много найдется людей, которые знали бы достаточно хорошо все эти отрасли? Лично мне, к счастью, повезло, у меня есть как раз эти три образования: электронное (Московский институт электронного машиностроения), финансовое (Финансовая Академия¹) и юридическое (юрфак МГУ). И верхнеуровневая проблема даже не в том, чтобы найти многопрофильных универсальных специалистов. Проблема в том, чтобы найти таких универсальных чиновников, потому что ведь именно они должны регулировать процессы на государственном уровне, в области публичного права, но в макроэкономических интересах, и опираясь на знания в области электроники.

РАЗБЕРЕМ СНАЧАЛА МАКРОЭКОНОМИЧЕСКИЕ РИСКИ

Первый риск — это риск недостаточной грамотности топ-менеджеров. Пример. На одной из профильных конференций выступил докладчик, занимающий весьма ответственную должность, который заявил, что блокчейн и биткоин — это совершенно разные вещи, к которым надо по-разному подходить. А вообще-то биткоин создан на технологии блокчейн. И ведь что интересно, никто не возразил, не возмутился, никто не зашикал...

Другой риск — недооценка будущего ущерба, возникающего в результате появления новых угроз в связи с развитием технологий, используемых в криминальных целях. То, насколько мы не понимаем будущие риски, можно проиллюстрировать таким примером. Лет пять назад все громко кричали: «Система „банк-клиент“ изменит жизнь, люди из дома по сотовому телефону будут высылать в банк платежки, и все будет хорошо». И никто не предупредил, что одновременно возникнут хакеры, которые будут взламывать счета, заходить туда вместо клиента, делать куда-то переводы. Это описывает Нассим Николас Талеб в книге «Антихрупкость»: «люди всегда говорят про высоту гор, исходя из

Риски	Пример	Конкретика
Риск недостаточной грамотности топ-менеджеров. Требуется одновременное детальное знание IT, юридического дела и финансов	Крупный докладчик заявил, что Биткойн и blockchain разные технологии и разные сущности, крупный банкир определил существование возможности обучить гуманитариев матаппарату Искусственного Интеллекта	
Недооценки будущего ущерба, возникающего в результате появления новых угроз в связи с развитием технологий, используемых в криминальных целях	Онлайн-банкинг, биоиентификация	Никто не оценивает, насколько выросла угроза взлома финансовых сетей после реализованной операции по хищению из изолированной сети ЦРУ кибероружия. Возможно существование технологии взлома принципиально нового класса, неизвестное обществу. С Термен-орлом разобрались только через 10 лет.
Выбора авторитетного, но неподходящего решения	SET 1995	Можно вложиться в то, что будет плохо работать
Обеспеченность	Blockchain	Отсутствие экономического обеспечения
Признания технологии лицензируемой или запрещенной к использованию и хранению, как уже было с наркотиками, оружием, алкоголем во время сухого закона	Биткойн, иные методы платежей анонимным бенефициарам	Wanna Cry, нанесший через британские больницы ущерб здоровью и жизни реальных людей, существует только потому, что не запрещен оиткойн и другие анонимные технологии платежей
Альтернативное денежное обращение, не контролируемое государством	Любые криптовалюты	
Неопределенность налогообложения обращения и прироста капитала		

Макроэкономические риски. Аналитики — ЦБ, Минторг

знания той самой высокой горы, которую они видели. Но это не значит, что они не найдут гору еще выше.» Никто не оценивает грамотно и квалифицированно вероятность риска того, что эти криптовалюты, не дай Бог, украдут. Недавно мне попала информация о том, что 10% денег, собранных при ICO, украдены хакерами. И это еще только начало. Процент похищенных средств будет расти, потому что хакеры быстро совершенствуются.

Другой пример. США - высокоразвитая страна, которая создает кибернетическое оружие для защиты своих интересов. И, чтобы заниматься этим оружием, ЦРУ разработало отдельную сверхсекретную сеть, физически не соединенную с остальным интернетом. И у них из этой сети это оружие украли! Возникает резонный вопрос: если хакеры смогли взломать изолированную сверхсекретную сеть ЦРУ в высокотехнологических США, неужели они не смогут взломать Центробанк? А ведь у криптовалют даже единого реестродержателя нет!

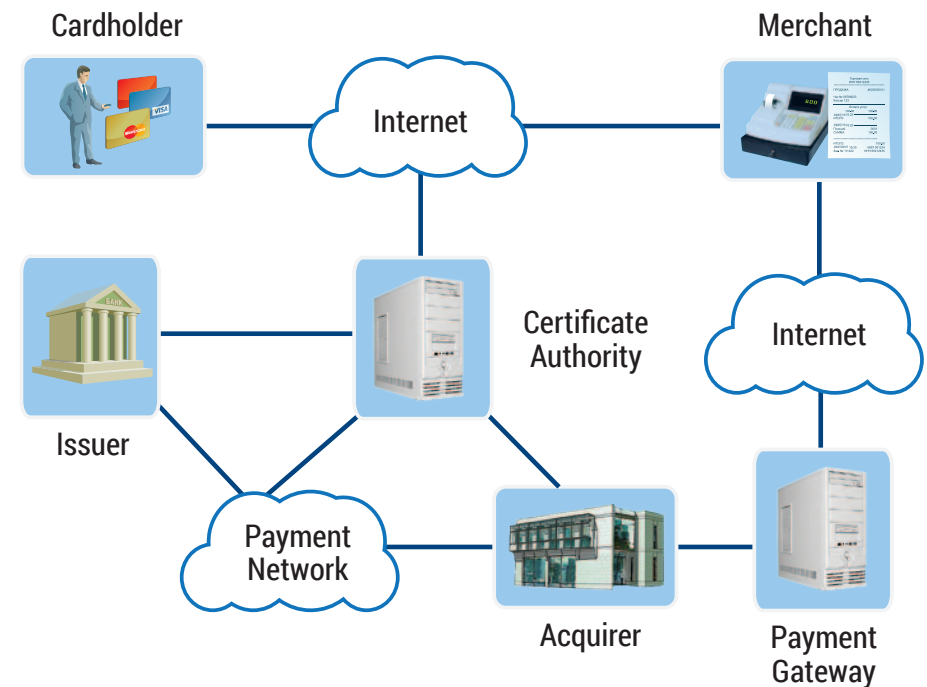


Есть очень показательная история о том, к чему приводит недооценка рисков технологий, про которые пока никто не знает. Российский изобретатель Лев Термен изобрел в свое время подслушивающую систему «Златоуст», которая потом 10 лет работала на Россию против американцев.²

Поехал как то американский посол в Артек, посмотреть на пионеров, и те подарили ему вырезанного из дерева орла. «Красивый орел, — подумал посол. — повешу у себя в кабинете, это же символ Америки. И потом, он абсолютно деревянный, никаких проводочков из него не торчит, электрическое питание не подведено, — там не может быть подслушивающих устройств!». Так орел 10 лет провисел у него в кабинете. И когда уже точно знали, что где-то у него в кабинете есть подслушивающее устройство, и разобрали всё по деталям, все-таки решили и этого орла посмотреть. Его разобрали и нашли некие проводочки. И оказалось, что если этого орла направленно облучать определенной радиочастотой, то проводочки выступают голосовым модулятором, которые берут звук и накладывают на эту частоту. А в другом месте эту модулированную частоту снимают с эфира и слышат, что говорится в кабинете.

Эта технология не была никому известна первые десять лет своего существования и использования. А вы представляете, сколько сейчас технологий, о которых мы не знаем,

а они есть, и они работают! Хорошо, если их когда-то вскроют и разрешат ими пользоваться. Вот, например, вы думаете, что купили мобильный телефон, и он ваш. А Наталья Касперская, говорит совершенно открыто³: «Смартфон — уже не ваше устройство. Вам его дают, чтобы вы побаловаться могли. А на самом деле это устройство совершенно других людей, которым мы передаем большой и теплый привет». Соответственно, мы совершенно не понимаем риски новых секретных технологий, именно в силу их секретности, а нам говорят — берите и пользуйтесь вовсю. А не прошло не только 10 лет, вообще почти нисколько не прошло.



SET components and Participants

Следующий макроэкономический риск — это *риск выбора авторитетного, но неподходящего решения*.

В 1996 году собрались монстры экономики — Microsoft, IBM, Visa, Mastercard и решили разработать единое для всех решение по электронным платежам. Разработали, называлось оно SET (Secure Electronic Transaction). Visa сказала: отлично, будем жить с этим решением. А грамотные люди, которые разбирались в ИТ, сразу поняли, что оно очень тяжелое, неудобное, и никто, условно говоря, не будет ездить в булочную на БЕЛАЗе. А те, кто не разбирались в ИТ (и в тот момент это был, в частности, Альфа-Банк), взяли и купили решение SET за сумму около миллиона долларов.⁴ Но уже через год поняли, что на БЕЛАЗе действительно неудобно ездить в булочную, да и Visa вдруг вышла из этой ассоциации, и IBM сказала - извините, мы ошиблись...

Получилась ситуация, когда все выбрали, кто-то один вложил, а потом остальные дружно сказали — ой, это будет не так. Альфа-Банк после этого долго ругался с Visa. Кончилось все тем, что их в утешение взяли в какой-то наблюдательный совет.

Что в этой истории важно — выбрать неправильное решение могут и самые опытные люди. И кто нам доказал, что именно биткоин - правильное решение, если сейчас на рынке уже несколько тысяч криптовалют? И биткоин даже контрольный пакет уже не держит среди них!

Все это — макроэкономические риски, оценивать которые должен кто? Центробанк, Минэкономразвития, Минпромторг и иные государственные органы.

Еще один макроэкономический риск — признание технологии лицензируемой или запрещенной к использованию и хранению, как уже было с наркотиками, оружием, алкоголем во время сухого закона. В свое время я задался вопросом,



какая валюта самая лучшая. Набрал в «Яндексе» запрос «самая лучшая валюта» ... и знаете, что он мне выдал? Первой же ссылкой? «Самая лучшая валюта — это патроны. Один патрон — одна жизнь».

В ряде мест, где идет война, так и есть. И наши спецназовцы, кто в Чечне воевал, тоже это понимают. Там, где закона нет, оружие — лучшая валюта. Но как только появляется закон — свободное обращение оружия запрещают. Есть список вещей, запрещенных в цивилизованном мире к свободному обращению: наркотики, оружие, ракеты, определенные химические вещества... Бывает так, что долгое время что-то было легальным, а потом вдруг становится нелегальным. Достаточно вспомнить историю компании Бауер: она начинала с легального производства и продажи кокаина. Были даже кокаиновые капли в нос — народный комиссар здравоохранения Николай Семашко прописывал их членам Совнаркома.

Бауер процветал, а потом кокаин запретили к легальной продаже. Тогда они начали производить героин,⁵ пока его тоже не запретили.

В такой сфере, как обращение денег, на которую государство смотрит очень внимательно, ситуация, когда что-то из легального может стать нелегальным, крайне вероятна. Очевидно, что криптовалюта в каких-то странах будет признана легальной, а в каких-то нет. В каких-то странах её уже запретили. И даже если у нас пока может существовать целый Telegram-канал, где висят объявления о продаже квартир, машин и даже титановых месторождений за биткоины и иные криптовалюты, то остается открытым вопрос юридического оформления такой сделки. Как признать, что сделка состоялась, что деньги перешли от покупателя к продавцу? И начинаются чисто юридические риски - признание сделки незаконной, нелегальной, несостоявшейся, или еще хуже — притворной.

Не так давно по миру прокатился вирус-шифратор WannaCry, который привел к реальным человеческим жертвам, потому что он в том числе зашифровал компьютеры, отвечавшие за жизнеобеспечение людей в британских клиниках. А откуда он взялся? Первые дешифраторы работали на отмене этого шифра при условии оплаты через SMS. И когда этот канал оплаты вымогателям перекрыли, хакеры перестали их рассылать эти вирусы, перестали использовать этот инструмент. Можно сказать, что WannaCry основан на существовании анонимных криптовалют: если бы не было биткоина, не было бы экономического смысла

запускать вирус-шифратор. Поэтому если человечество захочет защититься от вирус-шифраторов, то придется отменить анонимные криптовалюты. Ведь сколько можно заразить электроники этими вирусами-дешифраторами, начиная от смартфонов и заканчивая системой вентиляции! И если, не дай Бог, кто-то будет пугать весь мир такими вирусами, вопрос о запрете криптовалют встанет моментально. А принимают эти решения люди, которым выгодно принять политически выгодное популистское решение.

Еще один макроэкономический риск — альтернативное денежное обращение, не контролируемое государством. Об этом уже говорила и Председатель Центрального банка РФ Эльвира Набиуллина, и замминистра финансов Алексей Моисеев: ни одно нормальное государство не допустит на своей территории обращения валюты, которое оно не контролирует. До каких-то пределов на это не обращают внимания, но, как только объемы обращения вырастут - ситуация изменится.

Неопределенность налогообложения обращения криптовалют и прироста капитала. Буквально завтра государство может ввести любые налоги на криптовалюту, и такой риск тоже нужно предусмотреть.



КРИМИНАЛЬНЫЕ РИСКИ

Таких рисков немало.

Любая криптовалюта находится под риском использования для неисполнения законодательства по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ).

Еще один риск - антигосударственная социальная инженерия. Что это такое? Допустим, люди получают анонимный email, призывающий: «Приди на Болотную площадь в такое-то время, получишь 1/10 биткоина». Сколько людей придет? Можно собрать очень большую толпу. И представим себе — эти люди пришли и получают новое сообщение: «А теперь перейдите через мостик и дойдите до Красной площади». Или до Манежной. Любой, у кого в руках есть эта технология, может манипулировать большим количеством жадных и глупых людей дистанционно.

Третий риск - использование несоответствия текущему законодательству в мошеннических целях. Например, смарт-контракты, на которых все основано, в Гражданском кодексе вообще не описаны. Электронная цифровая подпись описана, она там называется АСП. А что такое смарт-контракты, с юридической

Риски	Пример	Конкретика
Использования для неисполнения законодательства по ПОД/ФТ	Любые криптовалюты	Нет единого эмиссионного центра, не идентифицированы плательщик и бенефициар
Антигосударственной социальной инженерии	Любые криптовалюты	Оплата цветных революций
Использование несоответствия текущему законодательству в мошеннических целях	Blockchain	Смарт-контракты не соответствуют понятию АСП в ГК РФ
Воровства или публичности коммерчески значимой информации и коммерческой тайны или персональных данных	Blockchain	По определению вся информация о всех сделках и сторонах известна
Хищения	С бирж были украдены криптовалюты на сотни миллионов	Необходимы гарантии правоохранительных органов сохранности средств, а также ЦБ, ответственного за денежное обращение в стране
При этом мы не сможем обеспечить абсолютную надежность транзакций в силу того что если по какой-то причине 50% +1 валидатор криптовалюты скажут, что транзакция была, а на самом деле ее не было, у нас не будет никакой возможности это опровергнуть, — пояснил Моисеев		

Криминальные риски. Аналитики: МВД, ФСБ, Росфинмониторинг, ЦБ

точки зрения не знает никто, и если прийти с этим в суд, у суда нет никакой законодательной базы, а тем более практики, по которой надо принимать судебное решение. Вы обменялись криптовалютами, да, но судебной поддержки этого решения нет по определению. Чему равен этот риск? Надо оценивать, взвешивать его. Потому что правила игры могут изобрести такие, что ваши вложения в криптовалюту обесценятся мгновенно.

Еще один риск: воровство или публичность коммерчески значимой информации и коммерческой тайны или персональных данных. Здесь кроется беда всей технологии блокчейн. Все знают про все сделки сразу. Вы знаете персональные данные всех. Это напрямую противоречит закону «О персональных данных».

Риск хищения мы выше несколько обсудили - те самые 10%. Пока. Как сказал господин Моисеев: «Мы не можем обеспечить абсолютную надежность транзакций в силу того, что если по какой-то причине 50% + 1 валидаторов криптовалюты скажут, что транзакция была, а на самом деле ее не было, у нас не будет никакой возможности это опровергнуть». А если эти валидаторы еще и анонимны, то риск возрастает существенно.

Риск нахождения запрещенной информации в сети криптовалюты. Любой валидатор криптовалюты является хранителем всего архива данных сразу. Поскольку подавляющее число валидаторов не является профессионалами в области создания и контроля криптографического ПО, то они не могут даже понимать, что внутри архива может находиться что-либо постороннее. При этом Исследователи из университетов Аахена и Франкфурта обнаружили, что в сети биткоина помимо финансовой информации хранится около 1 600 других файлов. Среди обнаруженных файлов семь нарушают авторские права: в них содержатся отрывки из разных whitepapers, приватный ключ RSA, секретный ключ ПО и ключ ко взлому защиты от копирования DVD. Также блокчейн биткоина хранит свадебные фотографии и снимок людей с указанием их онлайн-псевдонимов. Среди файлов обнаружены копии дипломатических телеграмм США, утечка которых произошла через WikiLeaks в 2010 году, и новость о демонстрации в Гонконге в 2014 году, некоторые файлы в блокчейне биткоина содержат противозаконную информацию и 274 ссылки на подобные ресурсы, 142 из которых ведут на сервисы в Dark web.⁶

Риск контейнерности криптовалюты. Любая криптовалюта (токен) является криптоконтейнером. Получив ее, пользователь может знать лишь информацию, написанную на «стенке контейнера», ее название и номинал. Знать, что находится внутри криптовалютного криптоконтейнера, пользователь не может именно в силу зашифрованности. А внутри может находиться все что угодно: инструкции по терроризму или совершенно секретная информация. Или вредоносный код.

Например, в публичный блокчейн может писать неограниченный круг лиц, контроль доступа не производится, и нет совершенно никаких шансов, что не придет какая-либо запрещенная информация или вирус. И нет никаких сертифицированных или хотя бы доверенных средств, чтобы проверить, что находится в криптоконтейнере. Кроме того, многие криптовалюты предоставляют разработчикам открытый API для разработки своих токенов на основе «основной валюты». У разработчиков имеются все возможности добавлять в криптоконтейнер нелегальный контент, и его вряд ли кто-нибудь контролирует помимо самих разработчиков.

Был ли в истории прецедент реализации рисков в «непроверенном контейнере»? Да, был. В XIII веке хан Хубилай запустил относительно «скоростные» караваны по «Шелковому пути». Кто возражал тогда против этой новой, явно революционной технологии доставки грузов? Все были «за» и очень рады. Просто никто тогда не понимал, что вирус чумы, являющийся природным в Монголии, не стал успевать убивать караваны в пустыне Гоби, и эти самые караваны за счет увеличения скорости стали разносчиками чумы в Европе и Китае. Цена реализации риска тогда составила смерть половины населения Европы и двух третей населения Китая.

Какая «зараза» сейчас может находиться в этих криптовалютных криптоконтейнерах, мы не знаем. Очень несложно поместить туда зловредное ПО, похищающее информацию или инфицирующее критическую информационную инфраструктуру. Какова величина остановки критической инфраструктуры, мы сейчас понимаем?

ТЕХНОЛОГИЧЕСКИЕ РИСКИ

Откуда взялась технология блокчейн? Никто об этом не говорит. А ведь технология распределенного реестра известна не последние лет пять, которые о ней говорят, а лет 35–40. И использовалась она обычно для автоматизированных систем управления войсками, прежде всего для обмена тактической информацией. Представьте себе, что у вас 50 боевых юнитов, которые ведут боевые действия. И какой-то юнит — например, вертолет, который поднялся в воздух, что-то важное увидел, получил информацию. Эту информацию надо передать всем юнитам подразделения и командованию, чтобы каждый из них имел полную картину боя. Либо напрямую, либо по цепочке. Транзакция считается законченной, только когда эта информация

Риски	Пример	Конкретика
Непредназначенности для данного использования	Blockchain	Технология распределенных реестров необходима для АСУ войсками
Несоответствия поставленным задачам (излишняя публичность, низкая скорость)	Blockchain	Все видят все транзакции, скорость — 3 (максимум 5) транзакции в секунду существенно увеличена быть не может
Непрозрачного создания	Биткоин	Автора никто никогда не видел, неясен источник финансирования в 20 млн долл.
Первоначального использования технологии	Биткоин	Родился внутри Tor'a, тесно связанным с ФБР (http://www.cnews.ru/news/top/anonim_naya_set_tor_na_60_finansi_ruetsya), в магазине Silk Road, называемым Amazon или Ebay для нелегальных товаров

Технологические риски. Аналитики — крупнейшие существующие интеграторы с большим опытом внедрения, производители банковского софта, Минсвязь

доехала до каждого разрешенного абонента. Не с того момента, когда каждый узнал, а именно когда дал отклик, что получил. Если у вас 50 абонентов, передача данных происходит достаточно быстро. Но как только их становится тысяча, начинаются проблемы... До этого не дозвонился, с этим связь потеряна... А блокчейн изначально рассчитан на многие тысячи узлов валидации. Поэтому быстроедействие этой технологии составляет максимум 7 транзакций в секунду. Что это значит в сравнении? У нас в «Киберплате» штатная «скорострельность» 100 транзакций в секунду, пиковая — 500. В Сбербанке, предположу, штатная где-то 400, пиковая — 1500 транзакций в секунду. Это сколько нужно блокчейнов? Когда Герман Греф говорит о пользе блокчейна, я сразу начинаю прикидывать — сколько же ему их понадобится?

Риск несоответствия поставленным задачам. Что такое 7 транзакций в секунду? Это около 220 миллионов транзакций в год. А у нас население 140 миллионов! Это значит, что каждый из нас может сделать меньше ДВУХ транзакций в год! А если надо три, то третью надо еще год ждать. Если же вам нужно, к примеру, 300

транзакций, то извините, вы не доживете до их выполнения. Поэтому внедрение такой технологии в больших сообществах в принципе невозможно. А большие сообщества как раз и обслуживают банкиры, им это интересно. Когда компанией IBM была собрана первая серийная сотня компьютеров, один купил Пентагон, один — метеорологи, а остальные 98 — банки.

Был кейс один, когда группа разработчиков, услышав, что быстроедействие 7 транзакций в секунду — это несерьезно, собрала в одной комнате тысячу компьютеров, соединила их оптикой и добила 200–300 транзакций в секунду. Но распределенность реестра, если весь этот реестр находится в одной комнате, становится никакой. Потому что если ты хочешь распределить по земному шару этот реестр, то надо пользоваться всей системой связи: медь, воздух, и так далее. А на распределенной, по-настоящему распределенной сети, такой производительности быть не может. Для военных 7 транзакций в секунду приемлемы. А банкиров такое быстроедействие не будет устраивать. Эта технология изначально делалась не под это и не подходит под нынешнюю форму финансового рынка.

Потихоньку подходим к главному. Риск непрозрачного создания. Кто писал техзадание на создание этого софтвера? Кто принимал в работу? Кто писал структурный алгоритм? Кто принимал в эксплуатацию код? Кто проводил отладку?



Фото: Хакер.ру

Наталья Касперская первая публично заявила об этом, что нет никакого Сатоши Накамото, а за блокчейном стоит группа американских криптологов. Мы уже знаем, что технология распределенного реестра изначально использовалась в АСУ войсками довольно давно, и именно поэтому про нее ничего не писали в научных и научно-популярных журналах. А теперь мы узнаем, что кто-то где-то эту технологию уже использует. И явно он в ней разобрался в ней раньше. А в каком месте есть люди, которые разбираются в таких вещах? Очевидно, что это - Пентагон.

Теперь давайте вспомним, где впервые был использован биткоин? Есть такая анонимная сеть Tor, и в ней был онлайн-магазин Silk Road, который торговал наркотиками. Сеть Tor существует на анонимные пожертвования, но как ни странно, известно, кто является главным донором: это Федеральное бюро расследований США. И понятно, что взломать эту сеть нельзя, потому что нужно взломать пять серверов подряд... Если, конечно, все эти пять серверов не твои. А если они твои, все пять, ты читаешь всю эту переписку и принимаешь решения: вот этих мы посадим — обеспечим статистику, этих мы не сажаем, а смотрим, кто на них клюнет, этих не сажаем - они нам платят. Злые люди говорят, что так и была создана сеть Tor — определенными людьми для определенных людей.

А про Интернет-магазин Silk Road злые языки говорят, что когда ФБР ловит кого-то с наркотиками, оно что-то там сдает государству, а остальное, конфискует, продает налево, а где самый удобный магазин, где продать конфискует налево? Очень удобный инструмент для этого - Интернет-магазин. Если еще знать, что в США все сотрудники ФБР официально освобождены от ответственности за операции с наркотиками под предлогом «им приходится это делать, чтобы в ОПГ внедриться», то картинка вообще становится законченной. Сразу становится ясно, кто и как контролирует данный рынок. Но, сделав несколько оборотов «наркотики/оружие — биткоин», эти люди начали сбрасывать криптовалюту или менять ее на квартиры, машины, титановые месторождения и так далее. А поскольку у этих людей есть в арсенале множество журналистов, раздуть историю вокруг всего этого не стоило никакого труда.

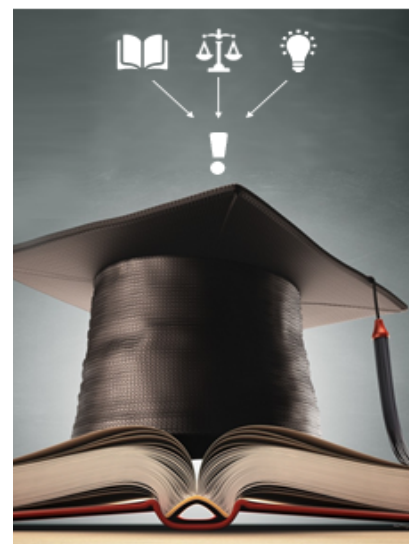
Прямым следствием всего вышеперечисленного является *Риск нечаянной утраты*. Доступ к кошельку с криптовалютой может быть утерян в результате потери пароля, сбоя на носителе данных, потере самого носителя данных.

Из-за принципа функционирования криптовалют и лежащей в его основе технологии блокчейна пароли пользователей нигде не сохраняются, кроме их памяти или личных записей. Нет соответствующего бизнес-процесса, при помощи которого можно в личном присутствии заменить пароли, удостоверить личность владельца и вернуть права на эти криптовалюты или иные криптоактивы.

Как сообщает New York Times, около 20% от существующих в мире 18,5 млн биткоинов находится на кошельках, которые были по какой-то причине заблокированы либо чьи пароли были безвозвратно утеряны. Общая стоимость валюты, которой нельзя воспользоваться, оценивается в \$140 млрд.¹

Подводя итоги. Перед тем, как куда-то войти, давайте подумаем — а как выходить будем? И если окажется, что это было отмывание в особо крупных размерах, то по сути вы оказываетесь соучастником отмывания операций с наркотиками и оружием.

ЧТО НАДО ДЕЛАТЬ



Направление принятия решений — разделение рисков по профилям

Соответственно, анализ рисков профильными специалистами

«Беда, коль сапоги начнет тачать пирожник»

Надо заняться менеджированием рисков. Описывается риск, описывается его максимальная величина, формируется так называемая стратегия угроз, описывается величина этой угрозы, и каким образом ей надо противодействовать.

Как известно, наиболее эффективными борцами с террористами являются сами террористы - те, которые контртеррористы. Они знают, каким образом осуществлять теракт, и легко догадываются, каким образом их можно нейтрализовать. Любой хороший изготовитель брони прекрасно знает, как устроен снаряд, иначе он не сделает броню. Почему, когда бандиты навязывают свою крышу, они называют это страховкой? Потому что это все единое целое.

Не так давно появилась теория государства как стационарного бандита, за нее чуть ли не Нобелевскую премию дали экономисту, который ее написал. Формулируя всю теорию в одной фразе — «у кого самая большая дубинка, тот и главный на этой территории». В случае с криптовалютами — то же самое. Чтобы заниматься макроэкономикой, нужно идти к крупнейшим жуликам в макроэкономике — в Центробанк, в Правительство. Чтобы заниматься криминалом, надо идти... понятно куда. Только тогда, когда им станет это выгодно и интересно, они начнут управлять этим процессом.

Мое глубочайшее убеждение, что настоящая Америка — та, которую мы знаем — началась с созданием в 1920-х годах Murder Incorporated. Когда крупнейшие мафиозные кланы собрались и решили, что убивать человека можно только с разрешения руководителей всех мафиозных кланов одновременно. Тогда кончился беспредел, и они своим внутренним судом приговаривали, кого можно убить, а кого нет. С этого момента страна стала цивилизованной. До этого ковбои стреляли по шерифам, а шерифы по ковбоям, и они друг от друга отличались только наличием или отсутствием значка. Но с того момента, когда в нелегальном пространстве появилось свое судопроизводство, с того момента началась цивилизация в США. Любой риск должен рассматриваться

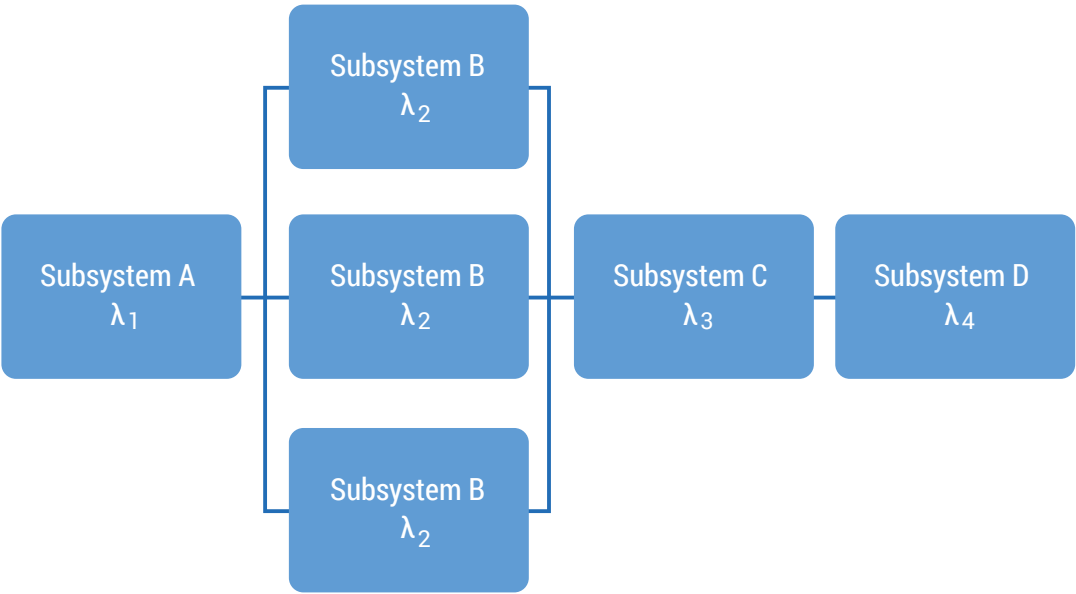
профессиональными риск-менеджерами. А вот кто они... Писать не будем, но понимать будем.

Поэтому для определения рисков криптовалют и создания риск-менеджмента криптовалют надо поделить все риски на группы, и каждую группу рисков должны изучить те, кто в этом разбирается.

- Например, IT риски стоит поручить Министерству связи и Академии Наук.
- Экономические риски — Центробанку, Минэкономразвитию, Минфину.
- Криминальные риски — Министерству юстиции, МВД, Прокуратуре, спецслужбам.

И только собрав профессиональные мнения всех групп воедино, можно принимать объединенное фундаментальное решение.

КАТАСТРОФОУСТОЙЧИВОСТЬ И ЖИВУЧЕСТЬ.



Теория вероятности учит нас, что двукратное дублирование информационной инфраструктуры в мирное время, например, на гражданских самолетах или в процессинговых системах, является вполне достаточным, а трехкратное уже и несколько избыточным. Называется этот параметр — катастрофоустойчивость. А вот в боевых самолетах и АСУ войсками, например, дублирование критической информационной инфраструктуры должно составлять 4–7 раз. По той простой причине, что во время использования этого устройства в боевых целях противник предпринимает меры для уничтожения такового. Поэтому при умышленном поражении 2–3–4 уровней боевой информационной инфраструктуры самолет или система управления все равно должны выполнять свои боевые задачи. Поэтому и уровень дублирования четырех-

семикратный. И называется это — живучесть. Термин этот используется при проектировании и тестировании оружия. Можно услышать словосочетания «живучесть корабля», «живучесть танка», «живучесть самолета». Но такого словосочетания для мирных систем нет. Потому что такой уровень живучести в мирное время не нужен. Не нужен для мирного пассажирского самолета семикратный уровень дублирования бортовой электроники. И для мирных процессинговых систем семикратный уровень дублирования тоже не нужен. Если, конечно, не ставить перед собой задач по финансированию терроризма, разведывательных сетей в тылу противника или осуществления заведомо противоправных деяний типа реализации наркотиков.

В блокчейне же каждый «добытчик» — «майнер» в идеале дублирует практически всю сеть. Это какая-то супермегаживучесть. Даже при уничтожении 99% резервирования блокчейн не перестает функционировать. Но разве возможно в мирное время потерять 99% инфраструктуры резервирования? Конечно, нет. Тогда зачем все время платить за такой явно избыточный ресурс?

За мегаживучесть криптовалют приходится платить дополнительной работой процессоров всех участников, а главное — временем транзакции. Именно явно избыточная мегаживучесть и является причиной низкой производительности и высокой ценой использования криптовалют.

Бывший генеральный директор PayPal Уильям Х. Харрис пишет «Требуется около часа для подтверждения транзакции биткойнов, а система биткойнов ограничена пятью транзакциями в секунду. MasterCard может обрабатывать 38 000 в секунду. Перевод 100 долларов США от одного человека другому стоит около 6 долларов США с использованием криптовалют и менее 1 доллара с помощью электронного чека... На создание одного Биткойна (процесс, называется «добыча») требуется столько же электроэнергии, сколько хватило бы средней американской семье на два года. Если бы биткойн использовался для значительной части мировой торговли (чего не произойдет), он потреблял бы очень большую часть мирового электричества, отвлекая дефицитную энергию от полезных целей».⁷

Для мирного применения блокчейна вполне достаточно сократить число узлов верификации до 10, максимум до 20. А если передать эти функции верификации игрокам, ответственным за риск-менеджмент данной криптовалюты, то все встанет на свои места. Получим сверхнадежную по катастрофоустойчивости (и даже живучести) платежную инфраструктуру, где верификаторами являются министерства и ведомства, уполномоченные государством. Риски использования такой криптовалюты будут минимальными.

Таким образом, наиболее рациональным развитием технологии распределенного реестра для создания криптовалют является создание криптовалюты с сильно ограниченным количеством верификаторов-реестродержателей, число которых, состав и обязанности (прежде всего по снижению рисков использования) будут определены Правительством. В их число обязательно будут входить Минсвязи, Академия Наук, Центробанк, Минэкономразвития, Минфин, Минюст, МВД, Прокуратура, спецслужбы.

Все остальные пользователи будут пользоваться этим реестром и не будут держать у себя «архивы» чужих транзакций.



Р. С.

В результате размышления и обсуждения систем распределенного реестра для систем автоматического управления войсками удалось понять, что число не только узлов дублирования, а даже абонентов у них, весьма ограничено. Во-первых, подразделение, грубо говоря, воюющее в районе Мурманска не нуждается в тактических данных на Кавказе. А во-вторых, при попадании в плен одного боевого юнита, противник не должен получить доступ к большому объему секретных данных. Что самое интересное, у диверсантов та же картина.

При попадании в плен одного диверсанта местная контрразведка не должна получить много информации о диверсионной сети. Число узлов дублирования, таким образом, даже в самых рискованных зонах не превышает 10.

То есть эмпирические данные дают нам возможность сделать вывод, что дублирование более 10 раз не нужно нигде и никому ни при каких условиях. Ни одному пользователю в мире. Закрытый интервал от 1 до 10. Не существует такого риска в природе, требующего более чем 10-кратного резервирования.

Тогда кому же нужны криптовалюты с многотысячекратным дублированием всего реестра?

При длительном размышлении удалось выявить только один тип организаций, которым надо знать все обо всех. Нет, конечно, есть еще и журналисты, но высокоуровневая криптография с элементами технологий систем автоматического управления войсками — это «не их почерк». Понятно, что для спецслужб, если они являются организаторами внедрения криптовалют, такой инструмент удобен. Каждый сам дает на себя весь объем частных данных, свято веря, что система анонимна, и не желая думать, что любой криптософт, созданный спецслужбами, просто обязан иметь «бэкдор».⁸

Это нормальная работа спецслужб, им именно за это зарплату платят. Но пользователям-то это зачем? Даже если у них есть такая большая любовь к спецслужбе своей страны, то можно, наверное, найти менее затратный и сложный метод передачи им информации. Если же речь идет о спецслужбе другой страны, то можно попасть в весьма щекотливую ситуацию, незамысловато описанную Уголовным Кодексом. Как писал поэт «там просто без соли едят, там штемпель ставят наугад, кладут в конверт и посылают за можай». И если домохозяйка сможет доказать твердое незнание основ теории надежности как части теории

вероятности, то любому айтишнику, который наверняка должен был ходить на лекции по терверу (теории вероятностей), да еще и экзамены сдавал, о чем осталось документальное подтверждение, отвергаться будет нелегко. Аргумент «все так делают» может и не сработать, поскольку гносеология — наука о познании, являющаяся частью философии, прямо говорит нам, что «мнение большинства не является критерием истины».

ЮМОР ПРО КРИПТОВАЛЮТЫ

При майнинге бульбы осуществляется тот же процесс — самозарождение ликвидной стоимости в результате многократной дубликации и репликации генетического кода картофеля.

Процесс майнинга картофеля сейчас более выгодный, чем майнинг биткоина. «Ферма» и участок 10 «соток» стоят одинаково, около 3000 у.е. С десяти соток хороший трейдер намайнит форк в восемь тонн бульбы, что по нынешнему биржевому курсу к доллару эквивалентно 2400 долларов США. Окупаемость проекта составит 15 месяцев. А если ферму подрагогнуть на навозе, то можно и все десять тонн собрать.

И при этом процесс майнинга бульбы идет без расходов на электричество, а сама майнинговая бульбо-ферма не теряет в цене.

Более того, у бульбы имеется побочный форк под названием «самогон». Перемайненные на самогон восемь тонн бульбы дадут полторы тысячи поллитров, или 7500 долларов США. Биткоин столько не принесет.

Ссылки

1. Ныне Университет
2. <https://geektimes.ru/company/pult/blog/281704/>
3. <https://www.computerworld.ru/news/Natalya-Kasperskaya-zayavila-chto-bitkoin-razrabotan-amerikanskimi-spetssluzhbami>
4. <https://alfabank.ru/press/news/2002/2/5/1.html>
5. <https://ru.wikipedia.org/wiki/Героин>
6. <http://bankir.ru/novosti/20180321/issledovanie-v-seti-bitkoina-obnaruzhen-zapreshchennyi-kontent-10137403/>
7. <https://www.recode.net/2018/4/24/17275202/bitcoin-scam-cryptocurrency-mining-pump-dump-fraud-ico-value>
8. <https://vz.ru/news/2018/7/15/932555.html>

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

«КИБЕРПЛАТ» (CYBERPLAT®)

Подписано в печать 10.12.2020. Формат 70×100/16
Гарнитура Cambria. Бумага офсетная. Усл. печ. л. 20
Тираж 300 экз. Заказ № 00000

Не для продажи

https://www.cyberplat.ru/download/Book_Cyberplat_epub.epub
https://www.cyberplat.ru/download/Book_Cyberplat.pdf

Отпечатано в АО «Первая Образцовая Типография»
Филиал «Чеховский Печатный Двор»

142300, Московская область,
г. Чехов, ул. Полиграфистов, д. 1
<https://www.chpd.ru>
e-mail: sales@chpd.ru
Тел.: 8 (499) 270-73-59